SIGNAL CORPS AND MILITARY INTELLIGENCE OFFICER PERCEPTIONS OF A MULTIFUNCTIONAL BRANCH MERGER

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

JOHNATHAN P. MARTIN, MAJOR, U.S. ARMY
B.F.A., Appalachian State University, Boone, North Carolina, 2003

Fort Leavenworth, Kansas
2015

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
12-06-2015	Master's Thesis	AUG 2014 – JUN 2015

4. TITLE AND SUBTITLE

Signal Corps and Military Intelligence Officer Perceptions of a Multifunctional Branch Merger

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Martin, Johnathan P. Major US Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

How the creation of the Cyber Branch will effect the Signal Corps and Military Intelligence branches is unclear. Budgetary factors are reducing Army end strength and increasing competition for the resources across the Department of Defense. These budgetary forces are likely to drive a search for efficiency. How the Army will transform to confront cyber threats while dealing with budgetary pressures is uncertain. One past solution was multifunctionalization. The multifunctional logistics program started in 1992 to reduce redundancy amongst the logistics branches, eventually becoming the Logistics Branch. Army leaders may view a similar approach to Signal, Military Intelligence and Cyber officer management as a way to reduce redundancy and cost. This research intends to access how Signal and Intelligence officers perceive a multifunctional merger of the Signal, Military Intelligence, and Cyber branches? The officers surveyed view the creation of the Cyber Branch as being positive for the Army. Most respondents would disagree with a merger of the Military Intelligence with any other branch. Conversely the majority of survey participants would support a multifunctional merger of the Signal Corps and Cyber Branch. Based on this research it is recommended that the Army consider a pilot volunteer program similar to the FA90 (Multifunction Logistician) for interested Signal and Cyber officers.

15. SUBJECT TERMS
Cyber, Signal, Intelligence, Branch Merger, Multifunctional, Officer Perceptions, OPMS, Officer Management, Cyber Branch, Cyber Organization, Signal Corps, Military Intelligence

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	113	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Major Johnathan P. Martin

Thesis Title: Signal Corps and Military Intelligence Officer Perceptions of a Multifunctional Branch Merger

Approved by:

_____, Thesis Committee Chair
DeEtte A. Lombard, M.A.

_____, Member
Timothy Hentschel, Ph.D.

_____, Member
Major Dennis J. Utt, M.S.

Accepted this 12th day of June 2015 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

SIGNAL CORPS AND MILITARY INTELLIGENCE OFFICER PERCEPTIONS OF A MULTIFUNCTIONAL BRANCH MERGER, by Major Johnathan P. Martin, 113 pages.

How the creation of the Cyber Branch will effect the Signal Corps and Military Intelligence branches is unclear. Budgetary factors are reducing Army end strength and increasing competition for the resources across the Department of Defense. These budgetary forces are likely to drive a search for efficiency. How the Army will transform to confront cyber threats while dealing with budgetary pressures is uncertain. One past solution was multifunctionalization. The multifunctional logistics program started in 1992 to reduce redundancy amongst the logistics branches, eventually becoming the Logistics Branch. Army leaders may view a similar approach to Signal, Military Intelligence and Cyber officer management as a way to reduce redundancy and cost. This research intends to access how Signal and Intelligence officers perceive a multifunctional merger of the Signal, Military Intelligence, and Cyber branches? The officers surveyed view the creation of the Cyber Branch as being positive for the Army. Most respondents would disagree with a merger of the Military Intelligence with any other branch. Conversely the majority of survey participants would support a multifunctional merger of the Signal Corps and Cyber Branch. Based on this research it is recommended that the Army consider a pilot volunteer program similar to the FA90 (Multifunction Logistician) for interested Signal and Cyber officers.

ACKNOWLEDGMENTS

This research thesis was made possible through the combined efforts and support of a great deal of people. This research simply would have not been possible without the support of the researcher's family, peers, instructors, and mentors. Only by the valuable support and input from these persons has this research been successfully completed. The researcher would like to use this opportunity to thank them.

First the researcher would like to thank his family for their support through late nights and weekends. Laura, Talmadge, Hunter and Madison Martin's undying support for this work has been admirable. I love you and appreciate your support.

The researcher would also like to thank the thesis committee members past and present, especially the committee chair Mrs. Deette Lombard. Your guidance and motivation throughout this research has been invaluable. The researcher would also like to thank the committee readers, Doctors Timothy Hentschel and Michelle Miller and Major Dennis Utt, this research would simply not have been possible without your feedback. The researcher is forever in gratitude to you all.

Doctor Maria Clark and the staff in the Command and General Staff College's Quality Assurance Office were essential in advising the construction and administration of the survey instrument.

The staff at the Ike Skelton Combined Arms Research Library was phenomenal in providing research assistance. They are an excellent resource for the Combined Arms Center and Fort Leavenworth community.

Finally the researcher would also like to thank his peers and the participants in the research study for their support and commitment to expressing their unvarnished opinions. You all have made this research a possibility.

TABLE OF CONTENTS

Page

ACRONYMS

ABCT	Armored Brigade Combat Team
AR	Army Regulation
ARCYBER	Army Cyber Command
BCT	Brigade Combat Team
BRAC	Base Closure and Realignment Report
BSB	Brigade Support Battalion
CAB	Combined Arms Battalion
CASCOM	Combined Arms Support Command
CEMA	Cyber Electro-Magnetic Activities
CGSC	Command and General Staff College
CI	Counter Intelligence
CLC3	Combined Logistics Captain's Career Course
CLOAC	Combined Logistics Officer Advanced Course
COCOM	Combatant Command
CoE	Center of Excellence
COSCOM	Corps Support Command
CPT	Cyber Protection Teams
CSA	Chief of Staff of the Army
CSB	Corps Support Battalion
DA PAM	Department of the Army Pamphlet
DCO	Defensive Cyber Operations
DISCOM	Division Support Command
DoD	Department of Defense

DoDIN	Department of Defense Information Network
DOIM	Directorate of Information Management
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities
EMS	Electro-Magnetic Spectrum
EW	Electronic Warfare
FA	Functional Area
FM	Field Manual
FSB	Forward Support Battalion
FSC	Forward Support Company
FY	Fiscal Year
GEOINT	Geospatial Intelligence
GIG	Global Information Grid
GWoT	Global War on Terrorism
HRC	Human Resource Command
HUMINT	Human Intelligence
IAVA	Information Assurance Venerability Assessment
IBCT	Infantry Brigade Combat Team
ICT	Integrated Concept Team
IDA	Institute for Defense Analyses
IDC	Information Dominance Corps (Navy Specific)
INFOSEC	Information Security
JNN	Joint Network Node
KD	Key Developmental
LG	Logistics Branch

MASINT	Measurement and Signature Intelligence
MC3	Maneuver Captain's Career Course
MI	Military Intelligence
MMAS	Master of Military Art and Science
MOS	Military Occupational Specialty
MSB	Main Support Battalion
NSS	National Security Strategy
OCO	Offensive Cyber Operation
OCS	Officer Candidate School
OD	Ordnance Branch
OPMS	Officer Personnel Management System
ORSA	Operations Research—Systems Analysis
OSINT	Open Source Intelligence
PME	Primary Military Education
QAO	Quality Assurance Office
QDR	Quadrennial Defense Review
QM	Quartermaster Branch
ROTC	Reserve Officer Training Corps
SBCT	Stryker Brigade Combat Team
SC	Signal Corps
SIGINT	Signals Intelligence
SOCOM	Special Operation Command
TC	Transportation Corps
TECHINT	Technical Intelligence
TRADOC	Training and Doctrine Command

USCYBERCOM United States Cyber Command

USMA United States Military Academy

ILLUSTRATIONS

Page

TABLES

Page

CHAPTER 1

INTRODUCTION

> We need one team. We need to think of ourselves not as signals, not as intelligence, not as cyber, but instead as some kind of team that puts us all together.[1]
>
> — General Keith B. Alexander,
> *Signal Magazine, 2013*

Introduction and Background

On September 1st, 2014 the Secretary of the Army established the U.S. Army Cyber branch as an Army basic branch. This is the first new basic branch since 1987. The creation of the Cyber branch recognizes the growing importance of the cyber domain in both strategic guidance and operational reality. Since its inception in 2009, two basic branches have been involved in the creation of the Cyber branch, Military Intelligence, and the Signal Corps. The roles, responsibilities, and authorities for Cyber actions are not clearly delineated between the two branches, as both have a role within the Army's Cyber construct. Cyber operations are divided into two components: Offensive Cyber Operations (OCO) and Defensive Cyber Operations (DCO). OCO entail attacking enemy forces utilizing cyberspace while DCO are aimed at protecting the friendly forces network infrastructure and the access to cyberspace. Military Intelligence personnel enable the selection and targeting of adversary assets utilizing the cyber domain, and are thusly responsible for OCO. The Signal Corps is traditionally responsible for installing, operating, maintaining, and defending the computer and information network, activities

[1] Robert K. Ackerman, "Cyber Command Redefines the Art," *Signal*, June 1, 2013, accessed December 8, 2014, http://www.afcea.org/content/?q=node/11117.

collectively supporting DCO. The split between who is responsible for the offensive and defensive components of cyber operations is a major impediment to the Army operating in the cyber domain, because both components are operating without a distinct unity of effort. The scope of this problem is accurately described by researchers at the Army Cyber Institute; Todd Arnold, Rob Harrison, and Gregory Conti as they argue for the creation of a Cyber Branch: "The need for a unified cyber career path is driven by operational necessity and a demand for efficiencies: our nation faces a critical national threat in cyberspace while today's disparate cyber stakeholders duplicate resources, induce friction, and lack the strength of a unified team." The Cyber Branch was established to streamline cyberspace operations by consolidating offensive and defensive cyber operations under one branch. The draft addition to Department of the Army Pamphlet (DA PAM) 600-3, Version 4, published on August 21st, 2014 states that the "Unique purpose of the Cyber Branch . . . (is) to conduct defensive and offensive cyberspace operations." The draft addition to the regulation does not mention either the Signal Corps or Military Intelligence branches' traditional role in cyberspace, nor does it cover how Signal Corps and Military Intelligence officers will interact with the cyber component. A lack of clarity in how these officers fit into this new cyber framework calls the Signal Corps and Military Intelligence branches' roles within cyberspace into question. Additionally, the Voluntary Transfer Incentive Program (VTIP) initiated to build the cyber force, seeks applicants with skills overwhelmingly represented in the Signal Corps and Military Intelligence communities (computing background, networking experience, security clearance etc.) The focused selection of officers may also be disconcerting to those remaining in the traditional branches, and may lead to questions of

continued relevance. Little professional research has been conducted to quantify this assertion; however, branch leaders' comments speak to member's concerns. For example, the U.S. Army G6, Lieutenant General Robert Ferrell stated: "The Signal Corps will be enduring. It will not go away. You're still going to be required to build, operate, and defend the network. Without the network, without the Signal Corps you will not have cyberspace operations." The former commander of the newly christened Cyber Center of Excellence (formerly the Signal Center of Excellence), Major General LaWarren Patterson echoed a similar sentiment during an interview with C4ISR and Networks, an online industry publication of the Gannett Company, stating:

> All of this is being worked out to determine what is best for the Army not one or two specific branches, and thus the need for a Cyber Center of Excellence a CoE with force modernization proponent responsibilities over the whole of cyberspace operations. Signal has a rather interesting history having created and birthed several other major capabilities. Aviation, intelligence and meteorological services can trace their lineage back to the Signal Corps. Each of these, and others, were eventually divested from Signal and yet Signal remains as strong and relevant today as ever.[2]

The amount of attention from the Army's highest ranking Signal officers clearly indicates that they are concerned about their subordinate officers' perceptions surrounding the creation of the Cyber Branch. External budgetary factors also contribute to tension surrounding the genesis of Cyber. Stricter budgetary constraints[3] create increased competition for the resources across the Department of Defense (DoD). As dominance in

---

[2] LaWarren V. Patterson, "Army turning Signal Center of Excellence into Cyber CoE," *C4ISR and Networks,* Ed. Barry Rosenberg, August 25, 2014, accessed November 28, 2014, http://www.c4isrnet.com/article/20140801/C4ISRNET07/308010002/Army-turning-Signal-Center-Excellence-into-Cyber-CoE.

[3] David Alexander, "Big Budget Cuts Pose 'Tough, Tough Choices' for Pentagon: Hagel," *Reuters*, March 6, 2014, accessed November 29, 2014, http://www.reuters.com/article/2014/03/06/us-usa-defense-budget-idUSBREA2500W20140306.

the cyber domain is a stated national policy objective, the funding stream for this force is assumed to be at least temporarily secure.[4] The reduced budget limits the funds available for external contractor support, and is compounded by end strength reductions, limiting the total number of personnel (Soldiers or civilian contractors) available. Smaller budgets combined with force reductions will most likely drive a search for opportunities for greater efficiencies as a means to accomplish more with fewer personnel. How the Army will transform to confront increased cyber threats while dealing with these budgetary pressures is unclear. The Army has managed difficult problems before. As the Cold War wound down in the late 1980s and early 1990s, a demand for a "peace dividend" grew, and as a result the Army end strength was reduced by 39 percent.[5] Due to the pressures of reduced budgets and personnel constraints, the Army implemented a series of changes aimed at reducing redundancy and increasing efficiency.

One area transformed by the aforementioned constraints was logistics. The multifunctional logistics program started in 1992 and became the Logistics branch on January 1, 2008.[6] The multifunction logistics program was created to reduce redundancy amongst the logistics branches. Under the multifunction logistics program officers are branched as Ordnance, Quartermaster, or Transportation officers. Once they are

---

[4] Joint Chiefs of Staff, *Capstone Concept for Joint Operations: Joint Force 2020* (Washington, DC: Joint Chiefs of Staff, 2012), 2-3.

[5] Bernard Rostker, *Right-Sizing the Force, Lessons for the Current Drawdown of American Military Personnel* (Washington, DC: Center for a New American Security, 2013).

[6] Paul Boyce, "Army Anounces Logistics Branch," The Official Homepage of the United States Army, December 13, 2007, accessed October 29, 2014, http://www.army.mil/article/6566/Army_Announces_Logistics_Branch/.

promoted to Captain (CPT), officers attend a combined career course and become multifunctional logisticians. Multifunction logisticians are able to fulfill any of the logistics related functions. Presumably, the multifunctional logistics officers are more able to directly synthesize the three distinct functions when planning and executing logistics support requirements. Additionally multifunctional officers better fit the inherently "multifunctional" logistics battalions (Forward Support Battalions (FSB) Main Support Battalions (MSB) and Corps Support Battalions (CSB).[7] Army leaders may view a multifunctional approach to officer management as a way to reduce redundancy and cost. A multifunctional program may also increase the individual officer's flexibility and the ability to synthesize signal and intelligence operations within the cyber domain.

This research is intended to examine the human dimension relating to changes in the traditional branch structure. Specifically, this research will focus on Signal Corps and Military Intelligence officer perceptions of a multifunctional merger of the Signal Corps, Military Intelligence, and Cyber branches.

Research Question

This thesis addresses the following question: How would Signal Corps and Military Intelligence Officers perceive a consolidation of Signal, Military Intelligence, and Cyber branches into one multifunctional branch? Two secondary research questions support the primary research question. First, how do signal and intelligence officers

[7] Major Christopher L. Day, "Training for Transformation: When Should the Army Train Multifunctional Logistics?" (Master's thesis, Command and General Staff College, Fort Leavenworth, KS, 2003).

perceive the creation of the Cyber branch? Second, how do signal and intelligence officers perceive the long term relevance of their branches?

Assumptions

Several key assumptions inform this research. First, it is assumed that Signal Corps and Military Intelligence field grade officers have the experience and knowledge, including operational experience, institutional training or self-development to provide relevant feedback concerning their branch as it relates to the cyber domain. It is assumed that adversarial threats in the cyber realm will continue to increase and that the Army will seek some level of organizational change to counter these threats and dominate the cyber domain. It is also assumed that current budgetary constraints and force reductions are accelerating the search for efficiency.

Scope and Delimitation

This research is not intended to determine whether or not a merger of Signal Corps, Military Intelligence, and Cyber Branches should occur or how such a merger will occur. This research focuses on the officers' perception of a hypothetical merger of specific branches into one multifunctional branch. Due to cyber becoming a branch this year there are no cyber officers readily available for this study. The first group of cyber officers are being accessed and trained during the writing of this study. Thusly this research is limited to Signal Corps and Military Intelligence branch officers. This research is limited to commissioned officers and therefore does not address the perceptions of warrant officers, noncommissioned officers, or department of the Army civilians. The sample population consists of CGSC students at Fort Leavenworth. It is

acknowledged that the opinions of the sample population do not fully reflect the perceptions of the entire Army officer population. Having served as a Signal Corps officer the researcher has designed an instrument mitigating inherent bias as much as possible arising from this branch affiliation.

Significance of Study

Soldiers are the Army's most important asset. Largely a people centric business, the Army must consider the opinions and perceptions of its personnel in meeting future challenges. Failure to account for the opinions of personnel could result in less job satisfaction.[8] Reduced job satisfaction amongst officers is linked to lower retention rates as the most talented officers seek greater fulfillment in the civilian sector.[9] This study is significant to understanding how Signal Corps and Military Intelligence officers would perceive a change to the traditional branch structure. This study allows Army leaders to gain a deeper understanding of the impacts of organizational change on personnel. Additionally, this study provides more depth into the intangible, emotional underpinnings supporting the individual officer's perception of the future. Additionally the cyber domain and cyber force are increasingly the topic of academic writing within the Military Art and Science arena; however, the opinions of Signal Corps and Military Intelligence offers are rarely accounted for in this research. Ideally this study will inform the body of research regarding the management and professional development of the cyber force

[8] Major Stephen J. Kolouch, "Retaining Army Engineer Officers" (Monograph, School of Advanced Military Studies, Fort Leavenworth, 2010).

[9] Beverly C. Harris, "Perceptions of Army Officers in a Changing Army" (Research Report 1662, Army Research Institute for the Behavorial and Social Sciences, Alexandria, VA, 1994), 37.

including Signal and Military Intelligence officers. Finally, this research should be used to inform decisions concerning the future roles and responsibilities of Signal Corps and Military Intelligence branches as Army leaders codify the implications of a possible merger.

Summary and Conclusions

The Cyber Branch was created to confront the growing number of threats in the cyber domain. The creation of a separate Cyber Branch has implications for the roles and responsibilities the Signal Corps and Military Intelligence branches fulfill within the cyber domain. The paradigm shift caused by the creation of the Cyber Branch may also affect how Signal, Military Intelligence, and Cyber officers' careers are managed in the future especially as the Army attempts to streamline personnel cost in an increasingly resource restrained environment. Establishment of a multifunctional Signal, Military Intelligence, and Cyber branch is one method the Army may use to reduce redundancy and cost. Army leaders must consider the opinions of their officers to successfully enact any change to the Army's branch structure. Signal and Military Intelligence officer perceptions of a multifunctional approach to their branches, constitutes a key metric in deciding what the effects of such a change could be.

CHAPTER 2

LITERATURE REVIEW

This literature review is organized in three sections. First is an introduction to the cyber domain. This section contains a brief review of background information about the cyber domain and why it has been a catalyst for change within the DoD and Army. Next is a brief review of the current academic writing about how the DoD and Army could institute organizational change to better address threats within the cyber domain. The third section is focused on the concept and practice of multifunctionalizing forces within the Army, and how this concept could be applied to Signal Corps, Military Intelligence, and Cyber Branch officers.

The Cyberspace Domain

Key Cyber Related Terms

The preponderance of current cyber doctrine, especially as it relates to Offensive Cyber Operations (OCO), is classified in nature and not available for public release. For the purpose of this study the researcher did not review classified information. The Information provided is intended to provide the reader with a general background of the cyber domain, and to provide insight into the imperatives guiding the DoD response to cyber in the Operating Environment. First some key terms are critical to understanding what "cyber" is. Army Field Manual (FM) 3-38 Cyber Electromagnetic Activities frames cyber within the context of both cyberspace and the electromagnetic spectrum, utilizing the term Cyber Electromagnetic Activities (CEMA). CEMA is defined as: Activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both

cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system. Both FM 3-38 and Joint Publication 1-02 (JP) the *Department of Defense Dictionary of Military and Associated Terms* use the same definitions for cyberspace: A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers. FM 3-38 defines Offensive Cyberspace Operations (OCO) as: Cyberspace operations intended to project power by the application of force in or through cyberspace. FM 3-38 defines Defensive Cyberspace Operations (DCO) as: Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net centric capabilities, and other designated systems. JP 1-02 includes the term cyber counterintelligence, not mentioned in FM 3-38. Cyber counterintelligence is defined as: Measures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions. Essentially the term cyber is applied as a modifier to denote that the action, task, or mission occurs or functions within the amorphous Global Information Grid (GIG) or its military sub component the Department of Defense Information Network (DoDIN). Additionally FM 3-38 states that cyberspace and the Electro-Magnetic Spectrum (EMS) are part of the information environment which defines the information environment as; the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.

Nature of the Cyber Domain

Cyberspace is unique amongst domains in that it functions simultaneously across all other domains, land, air, maritime, and space, yet it is not bound to or confined by any of them. Cyberspace is not associated with a particular physical space in the traditional sense. It is also the only man made domain created and maintained specifically for the transfer of data. As such cyberspace has a larger and more integrated human and informational dimension than the other domains. Cyberspace functions as a decentralized system of interconnected systems which change and expand rapidly to form an amorphous network. The cyberspace domain utilizes both wired and wireless methods of data transport and thusly coexists within the elector-magnetic spectrum.10 Operations within the cyber domain are able to have physical effects within any of the other domains. Because of the unique nature of cyberspace actors within it have the ability to affect the other domains without having a physical presence. Figure 1 illustrates the interaction between the cyberspace domain and the traditional domains.

[10] Headquarters, Department of the Army, Field Manual (FM) 3-38, *Cyber Electromagnetic Activities* (Washington, DC: Headquarters, Department of the Army, 2014).

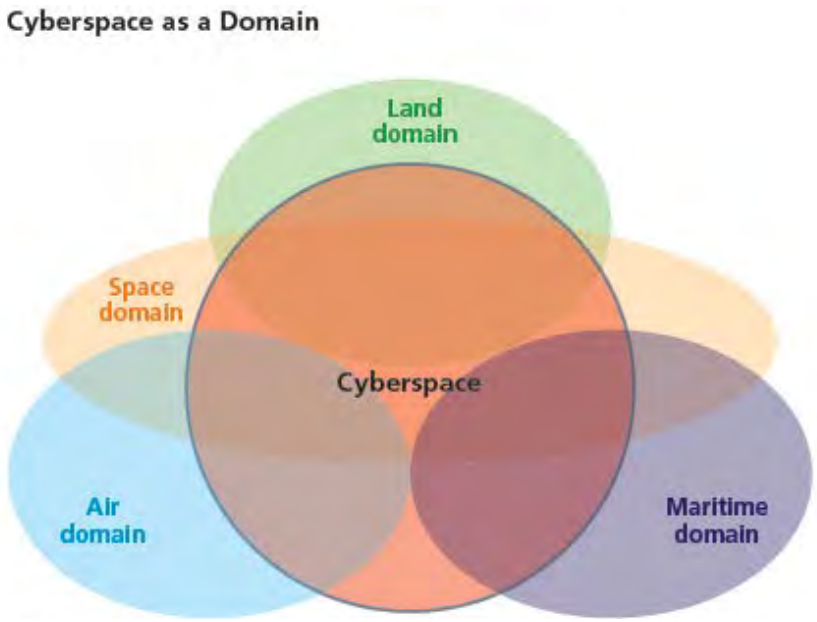


Figure 1. The Cyberspace Domain as it relates to the other Domains

Source: Isaac R. Porche III, Christopher Paul, Michael York, Chad C. Serena, Jerry M. Sollinger, Elliot Axelband, Endy M. Daehner, and Brudde J. Held, *Redefining Information Warfare Boundaries for an Army in a Wireless World* (Santa Monica, CA: Rand Corporation, 2013), 2.

Cyberspace is rife with both risk and opportunity for the DoD. Cyberspace is a driver of transformational change within the Army and greater DoD as they seek to minimize critical vulnerabilities while simultaneously leveraging expertise and technology to gain dominance of the cyber domain. Proficiency in cyberspace operations requires specific expertise, knowledge, and training. To gain cyberspace superiority The Army must acquire, develop, manage, promote, and retain proficient cyber operators. The next section of this chapter is a brief overview of the Army's officer management systems, and how the ascendancy of the cyber domain has altered them.

Organizational Concepts: how the Army Manages Cyber Personnel

The preponderance of recent academic writing on Army cyber focuses on how the Army should organize, manage, train and develop its cyber force. Most academic writing on the subject identifies four main concepts to potentially organize cyber forces:

1. Changing the branch structure to include a separately managed cyber branch,

2. Reorganizing the Officer Professional Management System (OPMS) categories, in a manner similar to the Navy's "Information Dominance Corps" concept,

3. Establishing a service like Combatant Command (COCOM), in a manner similar to the establishment of Special Operations Command (SOCOM) and,

4. Establishing a separate cyber service, in a manner similar to the creation of the US Air Force following the establishment of the Army Air Corps.[11]

The first portion of this section focuses on the first two organizational concepts (branches and the OPMS) because they are the most germane to the research question. For more information on a cyber service like COCOM construct see the Rand Corporation research report: *The Other Quiet Professionals: Lessons for Future Cyber Forces from the Evolution of Special Forces*,[12] by Christopher Paul, Isaac R. Porche III, and Elliot Axelband. For more information about a wholly separate cyber force see the detailed monograph by Air Force, Colonel Eric J. Denny entitled *The Cyberspace*

[11] The researcher arrived at this conclusion upon reviewing a variety of literary sources including those mentioned in the context of the paragraph. A list of sources reviewed based on the organizational principle they support is located in Appendix B at the end of this paper.

[12] Christopher Paul, Isaac R. Porche III, and Elliot and Axelband, *The Other Quiet Professionals: Lessons for Future Cyber Forces* (Santa Monica, CA: Rand Corporation, 2014).

Domain: Path to a New Service?[13] For a review of potential cyber organizational design evaluation criteria see "Does It Matter How the U.S. Army Organizes To Deal With Cyber Threats?"[14] by School of Advanced Military Studies (SAMS) graduate Major Shane A. Roppoli.

In addition to the overarching organizational constructs discussed several writers, such as Gregory Conti, Michael Weigand, Ed Skoudis, David Raymond, Thomas Cook, Todd Arnold and Daniel Ragsdale also highlight the need to address the talent management aspects of maintaining a cyber force within the currently fiscally constrained environment. Authors such as Colonel Maxwell Thibodeaux acknowledge that "in a severely constrained fiscal environment the Army may need to adopt an alternative that preserves its core missions and assets."[15] The two alternatives that Thibodeaux identifies are either the Army divests itself of the cyber mission and associated force, depending predominately on the Navy and (or) Air Force as the DoD's cyber proponent, or the Army establishes a "Multifunctional Information Corps."[16] A subsequent portion of this chapter will review the precedent for multifunctionalization set

[13] Eric J. Denny, Col., U.S. Air Force, "The Cyberspace Domain: Path to a New Service?" (Monograph, School of Advanced Military Studies, Fort Leavenworth, KS, 2013).

[14] Shane A. Roppoli, Maj, U.S. Army, "Does It Matter How the U.S. Army Organizes To Deal with Cyber Threats?" (Monograph, School of Advanced Military Studies, Fort Leavenworth, KS, 2013).

[15] Maxwell S. Thibodeaux, "Organizing The Army For Information Warfare" (Strategic Research Project, US Army War College, Carlisle, PA, 2013).

[16] Ibid., 25.

by the multi-function Logistics Corps, and identify other trends towards multifunctionalization across the Army and DoD.

Functional Branches: The Oldest Organizational Model

The Army utilizes a variety of structures to manage personnel within a logical framework. The Army's base organizational concepts are outlined in DA PAM 600-3 and serve the dual purposes of guiding officer professional development and informing Human Resource Command's (HRC) manning decisions. The oldest of Army organizational concept is the functional branch. The concept of branches dates back to antiquity when soldiers were trained and formed by their role (cavalry, light infantry, and archers). The branches continue to serve this function in the modern army where soldiers are developed, organized, and employed along a career path tailored to their branch specialty. Officers are assigned amongst seventeen Army basic branches, which are further grouped into categories, called career fields based on their respective functions.[17] According to the Chief of the U.S. Army Center of Military History, Force Structure and Unit History branch, Dr. Lewis Bernstein, the U.S. Army is representative of other western armies in its branch structure. The first branches have their genesis in the rudimentary adopted by the colonial militia. During the Continental Army period the branches were further refined along the lines of the French who advised the Continental Army during the Revolutionary War.[18] The Army has added and deleted branches as

[17] Headquarters, Department of the Army, Department of the Army (DA) Pamphlet 600-3, *Commissioned Officer Professional Development and Career Management* (Washington, DC: Headquarters, Department of the Army, 2010).

[18] Dr Lewis Bernstein, email received by author, January 30, 2015.

needed to fill known or anticipated capability gaps[19] and to incorporate new technical or technological advancements. The branch concept can be viewed as an extension of the functional view of capabilities western militaries use to organize their personnel and procurement processes. Researcher at the Institute for Defense Analyses (IDA), Kenton G. Fasana[20] identifies a couple of distinct advantages to employing a functional capabilities model. First it provides the ability to quickly recognize redundancies across various military services. Second, viewing procurement and personnel processes through a capabilities based lens allows military leaders to utilize a common lexicon in communicating end states and goals across the defense establishment. The branch system provides a similar function for the U.S. Army, and in many ways the branch construct was the beginning of the capabilities based approach. In addition to the positive attributes identified by Fasana the branches simplify manning and procurement processes by categorizing personnel and equipment in such a manner that "capability gaps" are readily identified and filled. It is also possible that the functional capability construct may improve esprit de corps by creating discrete branch subcultures within the Army as a whole. Members may rally around their branch, improving morale. Admittedly this conclusion is largely anecdotal. Fasana identifies a key fault endemic to a functional capabilities framework stating that: "A significant shortcoming of functional capabilities processes is their failure to properly address covariances that occur among capability

[19] Major Bryan E. Denny, "The Evolution and Demise of U.S. Tank Destroyer Doctrine in the Second World War" (Master's thesis, Command and General Staff College, Fort Leavenworth, KS, 1990).

[20] Kenton G. Fasana, "Using Capabilities to Drive Military Transformation: An Alternative Framework," *Armed Forces and Society* 37, no. 1 (January 2011): 141-162, accessed November 10, 2014, http://afs.sagepub.com/content/37/1/141.

categories."[21] The branch system is similar here in that the traditional branch structure has difficulty in dealing with convergence points between the traditional branches. An example of this is the current convergence of Signal, Military Intelligence and Cyber branches which the director of the Army Cyber Institute, Gregory Conti referred to as the "existing stakeholders"[22] in cyber operations. Figure 2 from Todd Arnold, Rob Harrison and Gregory Conti's collaborative article entitled "Towards a Career Path in Cyberspace Operations for Army Officers" illustrates the overlapping nature of roles and responsibilities within the cyber domain.

[21] Ibid.

[22] Todd Arnold, Rob Harrison, and Gregory Conti, "Towards A Career Path In Cyberspace Operations For Army Officers," *Small Wars Journal,* August 18, 2014, accessed September 2, 2014, http://smallwarsjournal.com/jrnl/art/towards-a-career-path-in-cyberspace-operations-for-army-officers.

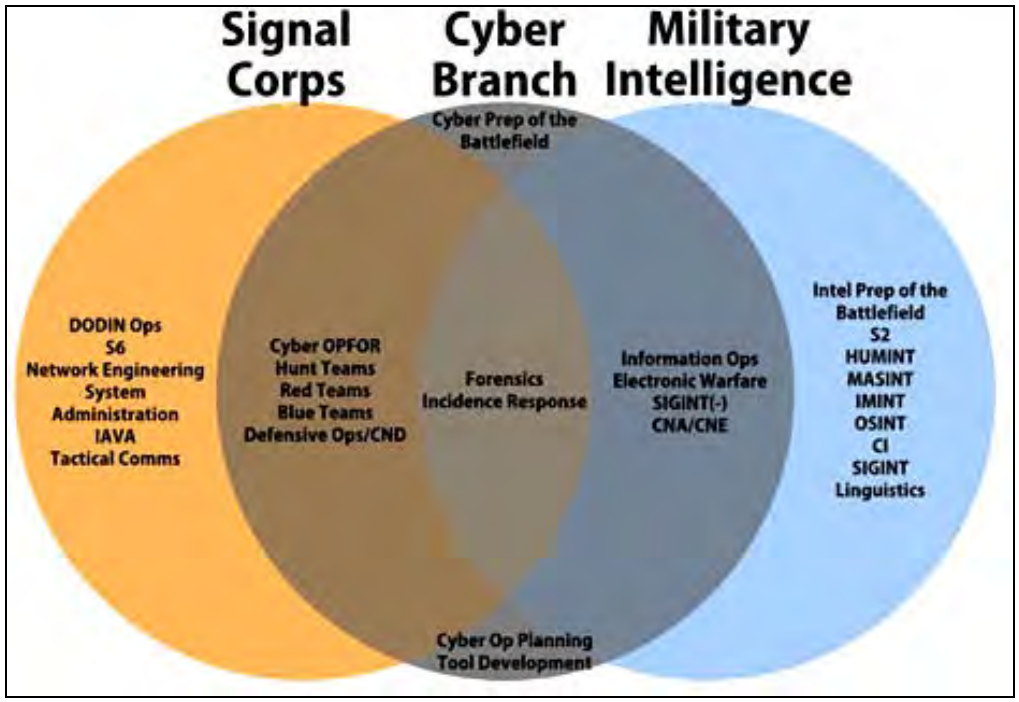


Figure 2. Proposed division of Labor between Cyber, Signal Corps, and Military Intelligence Branches

Source: Arnold Todd, Rob Harrison, and Gregory Conti, "Towards A Career Path In Cyberspace Operations For Army Officers," *Small Wars Journal,* August 18, 2014, accessed September 2, 2014, http://smallwarsjournal.com/jrnl/art/towards-a-career-path-in-cyberspace-operations-for-army-officers.

Similarly FM 3-38 lists the following staff elements as key in planning and coordinating CEMA operations: The Electronic Warfare (EW) Staff, Spectrum Manager, G2/S2 (Military Intelligence) and G6/S6 (Signal Corps). It is of note that EW is not a branch but a functional area (FA 29) and that the Spectrum Manager is a Signal Corps Soldier (MOS 25E). In effect FM 3-38 adds an additional element of complexity to the interrelationships between the various stakeholders in cyber, by including personnel associated with the EW, and electro-magnetic spectrum management fields. Figure 3 is a graphical representation of the elements supporting CEMA operations, including a

proposed delineation of roles and responsibilities inherent to the members of each branch. The overlapping areas existent between the various career fields represent potential friction points amongst the members of the CEMA team themselves, or their respective branches. As no one entity, or branch is given the primary authority or responsibility for the whole of CEMA operations infighting and competition for the resources allocated to CEMA operations is a distinct possibility.

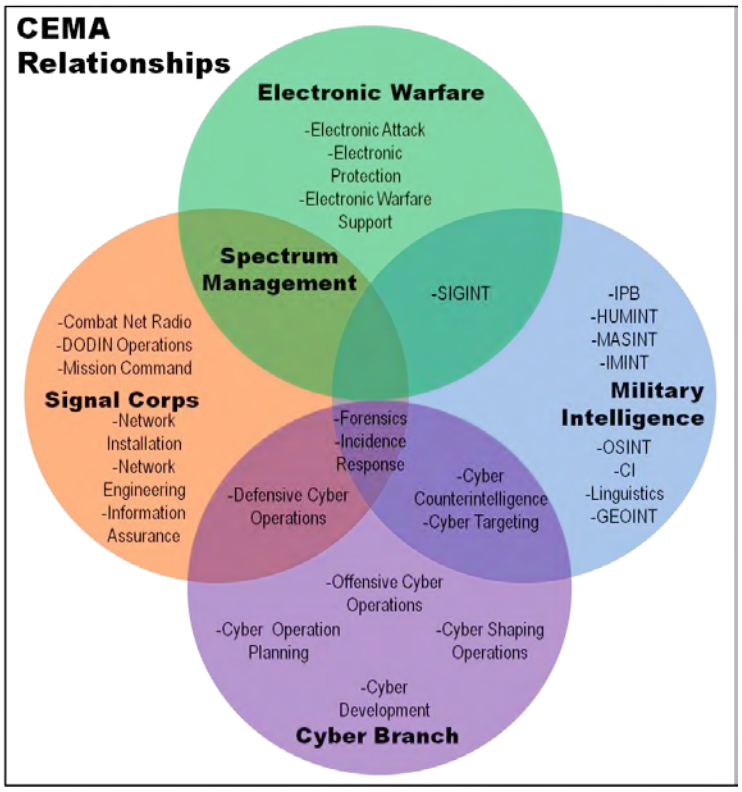


Figure 3. CEMA Element Concept Diagram

Source: Created by author.

The traditional branches may also have difficulty in the management of cyber talent. The fact that the first cyber operators belonged to either the Signal Corps or

Military Intelligence branches made it difficult for cyber leaders and HRC to effectively manage them. Compounding the difficulty of talent management, the Army's investment in terms of money and time is much greater for Cyber-related officers, effectively raising the stakes for personnel managers. The Army Cyber (ARCYBER) Commander, Lieutenant General Edward Cardon summed up the issue during a speaking engagement at CGSC stating: "We at the senior leader level are very concerned about retaining talented officers. . . . We are loosing people because we don't have a branch, right now they are Signal (Corps) or MI (Military Intelligence) and so Cyber guys have been subjected to the normal board process."[23] Cardon's comments highlight the difficulty in retaining personnel with discrete skill sets and training when the Soldiers themselves are limited to a prescribed career path designated by their basic branch. Not only might Signal Corps and Military Intelligence officers serving as cyber operators miss out on branch specific key developmental (KD) positions, they also may be passed over for promotion by a centralized board because they compete directly against other Signal Corps and Military Intelligence officers. The talent management aspect of the branch structure appears to be the impetus for creating a separate Cyber branch. Cardon said as much when he stated: "The most important part of cyber is the people. This is why we created a Cyber Branch; the people have to be managed. To make a really proficient cyber operator takes us five years."[24] To maintain a sufficient cyber force the Army invests significant resources to gain the human capital required and must safeguard its

[23] Edward C. Cardon, U.S. Army Cyber Command, "Cyber Briefing" (US Army Command and General Staff College, Fort Leavenworth, Kansas, December 3, 2014).

[24] Ibid.

investment. The creation of a separate Cyber branch is one way that the Army has acted to build capability in the cyber domain while simultaneously safeguarding its cyber operators from unplanned accessions. The creation of the Cyber Branch does not correct the disconnect between the Signal Corps and Military Intelligence branches operating within the cyber domain. More organizational shifts may be necessary, as Cardon said: "Signal and MI (Military Intelligence) are the big players in cyber. The MI (Military Intelligence) functions on the TS (Top Secret) side so they see a lot. The Signal guys function on the NIPR or SIPR at best so they see little. We're going to have to change the way we train our Signal operators to have the same knowledge as our offensive cyber operators."[25]

Finally a cultural friction also exists between the Signal Corps, Military Intelligence and Cyber operators (it is unclear what the Cyber Branch's organizational culture will be like at the time of this report). Cardon highlighted this issue during his speech, stating: "The Cyber (Branch) guys want to protect the network the Signal (Corps) guys are told: I don't care S6, make it work."[26] What Cardon is alluding to is the difference in culture stemming from the branches' particular mission sets. The Signal Corps has a culture dedicated to ensuring that communication occurs even if this entails some risk. The unofficial motto of the Signal Corps, "Get the message through" is representational of this mentality. Military Intelligence officers have a different branch culture. Military Intelligence culture is influenced by the demands of secrecy required of their job. As such Military Intelligence personnel participate in a culture which values the

[25] Ibid.

[26] Ibid.

safeguarding of information and compartmentalization.[27] As Cardon's comments indicate Cyber Branch officers will most likely create a culture that values protecting the network above providing increased access to it. These assertions are anecdotal as little to no research has been conducted into existing branch subcultures, or how they affect individual member interaction. The Central Intelligence Agency, Center for the Study of Intelligence researcher Dr. Rob Johnson's ethnographic study, *Analytic Culture in the US Intelligence Community* provides a theoretical basis to study Military Intelligence and perhaps other branches' cultures. There are no readily apparent solutions to bridge competing rather than complementary branch cultures. One bridging strategy is to place the members of the various cultures on the same "team" as the Army has done on a small scale with the CEMA concept, or how the Navy has done large scale with the Information Dominance Corps. The next section of this literature review reviews design strategies for managing groups of branches within the Army's Officer Personnel Management System (OPMS). By grouping officers from complementary fields into the same OPMS categories the Army may be able to close the gaps existing between the discrete branches.

Groups of Branches: the OPMS

The Chief of Staff of the Army from 1968 to 1972, General William C. Westmoreland identified a crisis of professionalism within the Army officer corps. As a result, Westmoreland tasked the Army War College to conduct "an analysis of the moral

[27] Dr. Robert Johnson, *Analytic Culture in the US Intelligence Community: Ethnographic Study* (Washington, DC: The Center for the Study of Intelligence, 2005). Dr. Johnson refers to this as a continuous competition between secrecy and performance.

and professional climate"[28] of the Army to access the potential factors contributing to this identified lack of professionalism. The War College Study found that the Army's officer personnel management policies had the unintended consequence of institutionalizing a negative organizational culture which favored self serving officers who focused on career advancement.[29] Westmoreland saw improving officer career management processes as critical to improving officer professionalism. The current OPMS is an evolution of the system that Westmoreland's Chief of Staff for Personnel, Lieutenant General Walter Kerwin Jr., implemented to address the Chief of Staff's concerns. The Army still utilizes the OPMS as an overarching capability based framework to manage officers through groupings of complementary branches and functional areas. DA PAM 600-3 the purpose of the OPMS is to:

> *Acquire.* Identify, recruit, select and prepare individuals for service as officers in our Army.
>
> *Develop*. Maximize officer performance and potential through training and education in accordance with AR 350–1, assignment, self-development and certification of officers to build agile and adaptive leaders.
>
> *Utilize.* Assign officers with the appropriate skills, experience and competencies to meet Army requirements and promote continued professional development.
>
> *Sustain.* Retaining officers with the appropriate skills, experience, competencies and manner of performance to meet Army requirements and promote continued professional development.

---

[28] William M. Donnelly, Ph D., "Professionalism and the Officer Personnel Management System," *Military Review* (May-June 2013): 16-23.

[29] Donnelly, "Professionalism and the Officer Personnel Management System"; U.S. Army War College, "Study on Military Professionalism" (U.S. Army War College Carlisle Barracks, PA, 1970).

Promote. Identify and advance officers with the appropriate skills, experience, competencies, manner of performance and demonstrated potential to meet Army requirements.

Transition. Separate officers from the Army in a manner that promotes a lifetime of support to the Service.

The OPMS has undergone several revisions; however its core functions of talent management and maintaining the Army's requirements for generalized and specialized officers remain the same. To accomplish its purpose the OPMS groups officers into career fields consisting of interrelated, supporting, or complementary branches and functional areas. Officers compete against others within their designated career group for promotion, and assignment to command selected positions. The career field categories have varied over time, shaping and reorganizing the officer corps. Figure 4 illustrates the various iterations of the OPMS' design through its evolution.

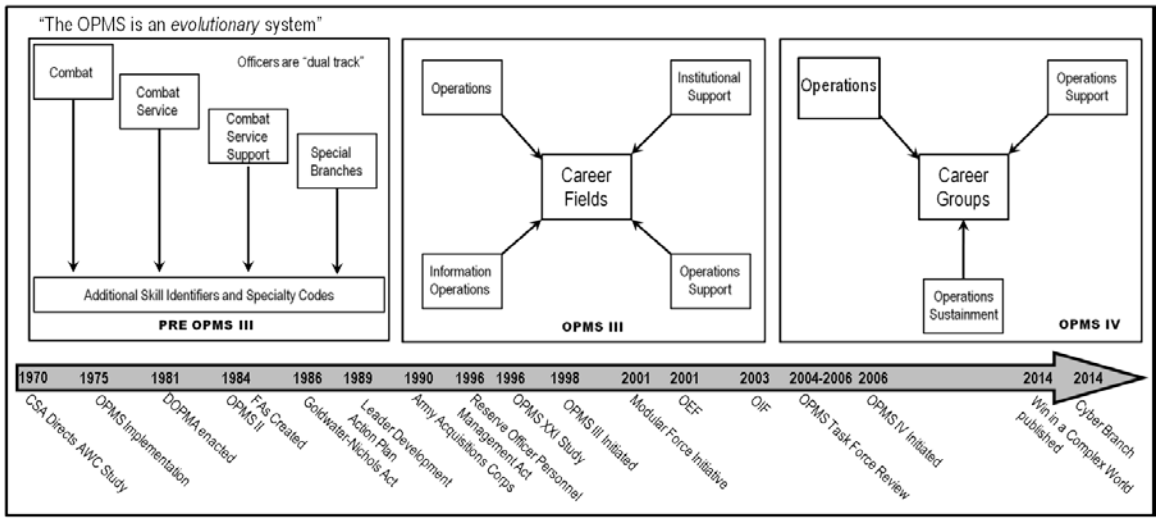


Figure 4. The Evolution of OMPS Design

Source: Created by author.

The search for an effective management solution for Signal Corps, Military Intelligence, and Cyber officers actually began as early as 1997. In 1997 OPMS III, and the OPMS XXI study which preceded it, grouped the following branches and functional areas together under the auspices of Information Operations career field: Signal Corps, Military Intelligence, FA24 (Telecom Engineering), FA30 (Information Operations), FA34 (Strategic Intelligence), FA40 (Space Operations), FA46 (Public Affairs), FA53 (Info Systems Management), and FA57 (Simulations). The concurrent version of DA PAM 600-3 described these officers as being "capable of integrating and optimizing the Army's relevant information, intelligence, information systems, public affairs, space operations and simulations to gain information dominance."[30] Similarly OPMS IV expands on the concept by increasing the number and type of officers within the Operations Support functional category. DA PAM 600-3(2 December 2014) list the following branches and functional areas together within the Operations Support functional category: Military Intelligence, Signal Corps, Cyber, FA53 (Information Systems Management), FA24 (Telecommunication Systems Engineer), FA40 (Space Operations), FA29 (Electronic Warfare (EW)), FA34 (Strategic Intelligence), FA48 (Foreign Area Officer (FAO)), FA59 (Strategic Plans and Policy), FA52 (Nuclear and Counterproliferation), FA50 (Force Management), FA49 (Operations Research—Systems Analysis), FA57 (Simulation Operations), FA47 (Permanent Academy Professor), and

[30] Headquarters, Department of the Army, Department of the Army (DA) Pamphlet 600-3, *Commissioned Officer Professional Development and Career Management* (Washington, DC: Headquarters, Department of the Army, 2005), 397.

FA46 (Public Affairs).[31]These officers are grouped together because the have "similar battlefield applications or complementary roles."[32] What the current OPMS is unable to do is to gain synergistic effects from grouping these officers together because as Army War College graduate Colonel Maxwell Thibodeaux points out:

> Information dominance is more than a machine-based affair . . . the Army must take into account the dynamic of information exchange. . . . It must not settle for networks and nodes. The common link between human and machine systems is the information itself, which transcends both the human dimension and the cyber domain.[33]

What Thibodeaux is suggesting is that the human dimension of the cyber domain holds the greatest opportunity for effectiveness both in execution of DCO and OCO. For example Thibodeaux points to the effectiveness of social engineering in enabling phishing attacks.[34] The human dimension may also be leveraged in conducting OCO by using human vulnerabilities to covertly introduce malicious code, as is suspected to be the case in the Stuxnet attack.[35]

Another difficulty for OPMS in managing Signal Corps, Military Intelligence, and Cyber Branch officers is meeting the officers broadening assignment goals. DA PAM 600-3 defines broadening as "a purposeful expansion of a leader's capabilities and

---

[31] Headquarters, Department of the Army, Draft Supplement to Department of the Army Pamplet 600-3, *Commissioned Officer Professional Development and Career Management* (Washington, DC: Headquarters, Department of The Army, 2014), 20.

[32] Ibid.

[33] Thibodeaux, "Organizing The Army For Information Warfare," 13.

[34] Ibid., 14.

[35] Kim Zetter, "An Unprecedented Look at Stuxnet, the Worlds First Digital Weapon," *Wired,* March 11, 2014, accessed January 21, 2015, http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

understanding provided through opportunities internal and external to the Army."[36] DA PAM 600-3 (December 2, 2014) indicates that broadening is a critical component of leader development stating: "The intent for broadening is to develop an officer's capability to see, work, learn and contribute outside each one's own perspective or individual level of understanding for the betterment of both the individual officer and the institution."[37] The fields represented in Operations Support are all specialized, as opposed to being generalist. Specialized officers often require more intensive specific training and certifications that take time. As they are focused on mastering and staying current in their functional specialty Operations Support officers may be less likely to meet the goals for broadening outlined in DA PAM 600-3. Officers who are generalist have another less tangible benefit, their ability to act as a connector between individual experts and/or groups of specialist. The generalist in the Army combines the talents of the specialist to ensure unity of effort.

Though the OPMS works reasonably well at managing the aggregate of Army officers it has significant shortcomings in conducting responsive talent management, establishing a unifying culture, and creating synergistic effects between groups of officers. Additionally the Operations Support designated branches are devoid of generalist, who if available could link disparate specialist or groups of specialist to gain the synergistic effects necessary to dominate the cyber domain. A multifunctional approach to the Signal Corps, Military Intelligence and Cyber branches may be a design

[36] Headquarters, Department of the Army, Draft Supplement to DA Pamplet 600-3 (2014), 20.

[37] Ibid., 23.

method the Army uses to gain synergy, unify cultures, and better manage talent. Multifunctional branches may also be seen as a way to gain efficiency, and reduce cost.

The Multifunctional Approach

Within the Army, multifunctional indicates the combining of functional capabilities, or responsibilities. The term multifunctional can be applied to units, such as the multifunctional logistics units (Brigade Support Battalions (BSB) and Forward Support Companies (FSC)) or to personnel such as multifunctional logisticians. Within the Army a multifunctional approach is most often associated with logistics; however other branches also exhibit some aspects of a multifunctional approach. This section describes the Multifunctional Logistics Branch and its progenitor, the multifunctional logistics program of 1992. This section also provides a brief overview of other current trends towards a multifunctional approach throughout the force.

Multifunctional Logistics

The impetus of multifunctional logistics began in the late 1980s. The Army experienced a budget reduction stemming from a massive modernization effort in the first part of the decade.[38] The fiscal environment led the Army to restructure in several ways such as lowering the number of combat divisions, and reducing overall personnel end strength. A component of the Army's restructure plan was to make logistics units multifunctional. Previously logistics units had a single specialized function, requiring a

[38] John V. Wemlinger, "The Army's Multifunctional Logistics Units: Can They Support The Joint/Combined Warfighting Effort?" (Report, The US Navy War College, College of Naval Warfare, Newport, RI, 1994).

division to field several different logistics units to provide its sustainment support.[39] The organizational change to multifunctional logistics units greatly reduced the size of logistics units, by consolidating headquarters and eliminating redundant capabilities. The movement towards multifunctional logistics began at the Division Support Command (DISCOM) level. The DISCOM was responsible for providing logistics support to the division's subordinate brigades. To accomplish this task the DISCOM was comprised of separate specialized battalions in the following logistics fields: maintenance, supply and transportation, and medical.[40] The DISCOM's functional battalion's task organized to support the maneuver brigades as the mission dictated. As author and retired US Army Colonel, John V. Wemlinger points out; the DISCOM was a fairly large organization in its pre-multifunctional guise, comprising nearly 2,500 Soldiers.[41] Under the improved organizational framework the Army was able to reduce the number of support personnel relative to the number of maneuver or combat personnel. Wemlinger surmises the benefits of multifunctional units well stating:

> First the Army was able to reduce the logistics side of its 'tooth-to-tail' ratio. Second, the Army correctly chose to reduce the total number of active duty divisions but kept the number of 'trigger pullers' in those divisions at a sufficient level. . . . A Forward Support Battalion (FSB) assigned to a DISCOM in a heavy division (that is a division with a mix of mechanized infantry and armor in the brigades) has 433 assigned personnel at strength-level one. A maintenance battalion in the functionally organized DISCOM of an infantry division had over 1000 personnel assigned. The significantly smaller number of personnel assigned to the FSB's when compared to the functional battalion represents the decrease in

[39] Ibid.

[40] Ibid.

[41] Ibid.

> the 'tail' side of the 'tooth-to-tail' ratio. The 'tooth' number has not changed in any of the Army's remaining ten active duty divisions.[42]

The new DISCOM battalions, christened Forward Support Battalions (FSB) and Main Support Battalions (MSB), were leaner than the organizations they replaced, but still needed to provide the same level of support to the same number of combat units. A significant change to the doctrine supporting sustainment operations was required to facilitate closing the sustainer to war fighter personnel gap. The improved doctrine emphasized habitual relationships between the FSB and supported brigade and between the DISCOM units and the higher echelon Corps Support Command (COSCOM).[43] Under the newer sustainment construct each level of support is dependant on a level of mutual support from a like unit at the next higher echelon. The first test of multifunctional logistics units was Operation Desert Shield and the subsequent Operation Desert Storm. Despite initial problems in planning the multifunctional units were able to support operations of an unprecedented scale, moving 500,720 passengers and 543,548 tons of cargo by air and 3,048,532 tons of dry cargo and 6,103,015 tons of petroleum by sea.[44] The multifunctional logistics units had passed the test; however the logisticians leading those formations remained specialized.

Though logistics units had changed the officers leading them were still trained and managed within their respective branches. The Army's sustainment structure lacked

---

[42] Ibid.

[43] Ibid.

[44] Lieutenant Colonel Joseph R. Kurz, "Sustainment Essentials of the Persain Gulf War," *Army Sustainment* 44, no. 1 (January-Febuary 2012), accessed Febuary 24, 2015, http://www.almc.army.mil/alog/issues/JanFeb12/Sustainment_Essentials.html.

officers who were generalist in the field of logistics. The Army's Combined Arms Support Command (CASCOM) (another product of the Army's realignment of sustainment forces, CASCOM was created in 1990 when the U.S. Army Logistics Center merged with the U.S. Army Soldier Support Center)[45] recognized the need for logisticians able to lead the multifunctional units and synthesize the separate sustainment functions. The CASCOM established the multifunctional logistician program and the Combined Logistics Officer Advanced Course (CLOAC) in 1992. In 1993 the Army adopted the program establishing the Functional Area (FA) 90, Multifunctional Logistics specialty. Officers in the Ordnance, Transportation, and Quartermaster branches could opt to become multifunctional logisticians. Upon accessing to FA90 these officers could fill roles coded as multifunctional in nature, or jobs within their previous logistics specialty. Additionally functional officers (those remaining in their basic branch) could be assessed as multifunctional by successfully filling FA90 qualifying positions. This process later became centrally managed by Human Resources Command (HRC) which convened boards to validate FA90 certification requirements were met prior to assigning lieutenant colonels to key logistics billets.[46] Multifunctional validation became more important as FA90 certification was a prerequisite for an increasing number of command assignments. Figure 5 illustrates the state of the logistics command slate in 2004.

[45] Combined Arms Support Command, "History of CASCOM," April 15, 2014, accessed Febuary 24, 2015, http://www.cascom.army.mil/about/history/index.htm.

[46] Terry E. Juskowiak, "FA90: An Update on the Multifunctional Logistician Program," *Army Logistician* (November-December 2004): 1-6.

LTC Command Selection List Migration

BR	Category	Title	Current	Proposed	MOS	Change
OD	6G	Ammunition	2	2	91	-
	6DR	Advanced Individual Training (AIT)	5	5	91	-
	6I	Explosive Ordnance Disposal (EOD)	4	4	91	-
	6KR	Ammunition Plant/Depot	5	4	91	-1
QM	6E	Supply – Tactical	2	0	90	-2
	6ER	Supply – Training Support System (TSS)/AIT	11	3	92	-8
	6G	Petroleum, Oils, and Lubricants (POL) – Tactical	2	2	92	-
	6GR	POL – TSS	3	3	92	-
TC	6F	Transportation – Tactical	14	14	88	-
	6LR	Surface Deployment and Distribution Command – TSS	12	0	88	-12
	6FR	AIT	3	3	88	-
FA 90	6S	FA 90 – Tactical	75	75	90	-
	6SM*	FA 90 – Materiel Management Center	0	2	90	+2
	6SR	FA 90 – TSS	8	10	90/88 88/92	+2
	6ST*	FA 90 – Surface Deployment and Distribution Command	0	12	90/88	+12

* Indicates new categories

Figure 5. LTC Command Selection List Migration

NOTE: This chart shows the changes in lieutenant colonel-level commands. Note that multifunctional commands requiring FA 90 are increasing and functional commands are decreasing.

Source: Terry E. Juskowiak, "FA90: An Update on the Multifunctional Logistician Program," *Army Logistician* (November-December 2004): 1-6.

The FA90 system continued in this same structural framework though academics and senior leaders within the Army's sustainment community debated the merits of a singular logistics corps. The adherents of the traditional branches advocated that expertise in a specified career field takes time to develop. Additionally tradition was firmly on their side with Quartermaster being amongst the original branches formalized by congress in the early 1800s. The 2002 publication of *The Path to Victory: America's Army and the Revolution in Human Affairs* by author and retired Major Don Vandergriff represented the opposite view. Among other radical personnel changes Vandergriff advocated reducing, or eliminating the Army's traditional branches as a means of providing more

flexibility in officer personnel management.[47] Regardless of their opinions many of the Army's thinkers were reassessing the traditional branch and officer personnel management structures. Though controversial the consolidation of the logistics branches and specialties was a real possibility given the fiscal and manpower constraints the Army was operating under. Major General retired Juskowiak was prophetic when he wrote the following for Army Logistician in 2004: "Now is the time, in this exciting period of transformation—when real change is being accomplished—to look hard at the logistics institutions and what they could and should look like in the next 10 to 15 years. A future force with one Army logistics corps may become a reality."[48] Little did he know that the events that would lead to the creation of the Logistics branch were underway.

In 2004 a review of officer personnel management policy by the Officer Personnel Management III (OPMS III) Task Force was initiated. As part of the task force's review of personnel management policies and procedures they recommended that a mono-lithic logistics corps be created.[49] The Chief of Staff of the Army (CSA) directed Training and Doctrine Command (TRADOC) to develop an implementation plan for creating a logistics corps. CASCOM took the lead in this task establishing an integrated concept team (ICT) comprised of the relevant stake holders to review how the CSA's guidance could be implemented utilizing the doctrine, organization, training, materiel,

---

[47] Donald E. Vandergriff, *The Path to Victory: America's Army and the Revolution in Human Affairs* (Novato, CA: Presidio Press, 2002).

[48] Ibid.

[49] Major Vickie D. Stenfors, "The Logistics Officer Corps: Growing Logistics Pentathletes for the 21st Century," *Army Logistician* 38, no. 5 (September-October 2006), accessed Febuary 24, 2015, http://www.alu.army.mil/alog/issues/SepOct06/pentathletes.html.

leadership and education, personnel, and facilities or DOTMLPF framework.[50] The former manager of the FA90 proponent, Major Vickie Stenfors summarizes the findings of the ICT in an article for *the Army Logistician*:

> [I]t became apparent that officers must be designated and trained as multifunctional logisticians earlier in their careers. Although approximately 60 percent of all logistics captain positions are currently functional [meaning single function, or specialized], this number is decreasing. By fiscal year 2008, 55 to 60 percent of all captain positions will be coded multifunctional. Over 60 percent of field-grade logistics officer positions are already coded multifunctional, and that number is growing. Officers from all three logistics branches (Ordnance, Quartermaster, and Transportation) in the ranks of captain to colonel serve in many multifunctional-coded positions throughout their careers. The analysis confirmed that, despite these statistics, there is a continuing need for functional expertise at all grade levels. Therefore, a way must be found to develop functional expertise in niche skills such as petroleum operations, strategic transportation, and explosive ordnance disposal.[51]

The CASCOM Commander briefed the ICT findings and recommendations to the CSA who approved the creation of the Logistics branch.

On January 1, 2008 the Logistics branch (LG) was created. This is an expansion of the previous FA90, multifunctional logistician career field to a branch covering all Army logisticians. The Logistics branch is not an initial assignment branch as newly commissioned second lieutenants are initially assigned to one of the traditional logistics career fields, Ordnance, Transportation, or Quartermaster. Officers become a member of the Logistics branch once they complete the Combined Logistics Captains Career Course (CLC3), a revision of the CLOAC. All logistics officers are now considered multifunctional prior to their company level command. Officers who had attended their

[50] Ibid.

[51] Ibid.

captain's career course but were not previously FA90 certified were automatically converted over to the Logistics branch on January 1, 2008.

The creation of the Logistics branch is unique in the Army's history. Previously the expansion of branches was favored often with one branch birthing another. The Military Intelligence branch was birthed from the Signal Corps for example. The Logistics branch represents the first time that branches have been consolidated in line with the officer's career development timeline. The logistics branch is not the only example of the Army leveraging a multifunctional approach.

Multifunctional Maneuverist

In 2010 the Armor School at Fort Knox, Kentucky was shuttered and moved to Fort Benning, Georgia, the former "Home of the Infantry." This move established the Maneuver Center of Excellence (MCoE) as the sole proponency for training and developing the Army's maneuver forces; the Infantry and Armor branches. This realignment was based on a recommendation from the 2005 Base Closure and Realignment Report (BRAC) which estimated that the move would save the Army over 948 Million dollars over the next 20 years.[52] Though not specifically stated as multifunctional in nature, this move has realized a gain in training efficiency similar to a multifunctional merger. In addition to the establishment of the MCoE the Maneuver Captains Career Course (MC3) was created to train and develop Infantry and Armor officers prior to company level command. Being that Armor and Infantry officers attend the same career course the positions available to Armor officers have also increased. DA

[52] Department of Defense, *Base Closure and Realighnment Report,* Volume 1, Part 2 of 2 Detailed Recommendations (Washington, DC: Department of Defense, 2005).

PAM 600-3 states the following: "Armor officers initially focus on development of the core technical and tactical Armor mobile protected firepower and reconnaissance and security skills. . . . Armor officers continually deepen their core skills while developing broader skills in combined arms maneuver, wide area security in support of unified land operations."[53] What this means in essence is that Armor officers are expected to have the same core competencies as their Infantry branch peers once they have moved beyond their initial skill level (second and first lieutenant level). Figure 6 illustrates the skill identifiers (SI) associated with the Armor and Infantry Branches.

Infantry Branch	Armor Branch
Infantry Branch is the proponent of the following SIs	**SIs associated with Armor AOCs:**
2B–Air Assault.	M1A2 Abrams Tank (3J).
3X–Bradley Leader.	**M2 BIFV/M3 CFV/M7 Bradley fire integration support team leader (3X).**
3Z–Mortar Unit Officer.	Stryker Leader Course (R4).
5P–Parachutist.	Army Reconnaissance Course (R7).
5R–Ranger.	**Ranger/Ranger-Parachutist (5R/5S).**
5S–Ranger/Parachutist.	**Airborne (5P).**
5Q–Pathfinder.	**Air Assault (2B).**
5W–Jumpmaster.	**Pathfinder (5Q).**

Figure 6. DA PAM 600-3 Skill Identifiers Associated with the Infantry and Armor Branches

NOTE: The skills expected of the officers of each branch are similar; those which are the same are indicated in bold.

Source: Created by author data from Headquarters, Department of the Army, Department of the Army (DA) Pamphlet 600-3, *Commissioned Officer Professional Development and Career Management* (Washington, DC: Headquarters, Department of the Army, 2010).

The net result of Armor officers receiving the same training as the Infantry counterparts is an increased assignment of Armor officer to traditionally Infantry units. Armor Branch officers can be assigned to Infantry Brigade Combat Teams (IBCT),

[53] Headquarters, Department of the Army, DA Pamplet 600-3 (2010).

Stryker Brigade Combat Teams (SBCT) or Armored Brigade Combat Teams (ABCT).[54] Once assigned these Armor officers can fill vacancies coded as 19A (Armor) or 02B (Infantry/Armor). Armor officers in the rank of Lieutenant Colonel may also command Combined Arms Battalions (CAB) and lead subordinate Infantry formations. Infantry and Armor officers are not yet multifunctional, but it could be argued that the Army is moving closer to the vision outlined by Don Vandergriff in 2002.

Summary

The Army has a variety of ways available to organize its cyber forces. The Army created the Cyber Branch in an effort to better manage cyber related officers; however as budgetary pressures continue to mount, the desire for increased efficiency is assumed to increase. The Army has a greater dependence on technology and mission command systems than ever before. Commanders at all levels have an insatiable appetite for information, surveillance, reconnaissance, and analysis to drive their operations. Threats within cyberspace are increasing at an exponential rate. The current and envisioned future operating environment seems to necessitate an increase in the quantity and quality of Signal Corps, Military Intelligence and Cyber officers. It is currently unclear how the Army will choose to organize its Signal Corps, Military Intelligence, and Cyber branches to handle the concurrent trends of growing threats, reduced budgets, and increased demand, but a multifunctional approach appears to be a plausible solution.

[54] Ibid.

CHAPTER 3

RESEARCH METHODOLOGY

Concept of Research

This research was designed as an exploratory ethnographic study to gain an understanding of how Signal Corps and Military Intelligence officers perceive a potential branch merger. The study is a qualitative in nature and focuses on the participant's individual perceptions in order to answer the research question and the two secondary questions. The data base was derived through an electronically administered questionnaire, conducted in February 2015. The participants were a purpose based sample of the resident students at the US Army Command and General Staff College (CGSC) at Fort Leavenworth, Kansas. Forty (40) students participated in this research. The selection of the data base was informed by a review of current and past academic writing on the subject and by analysis of senior leader speeches and interviews. A conceptual database design model is illustrated in figure 7.

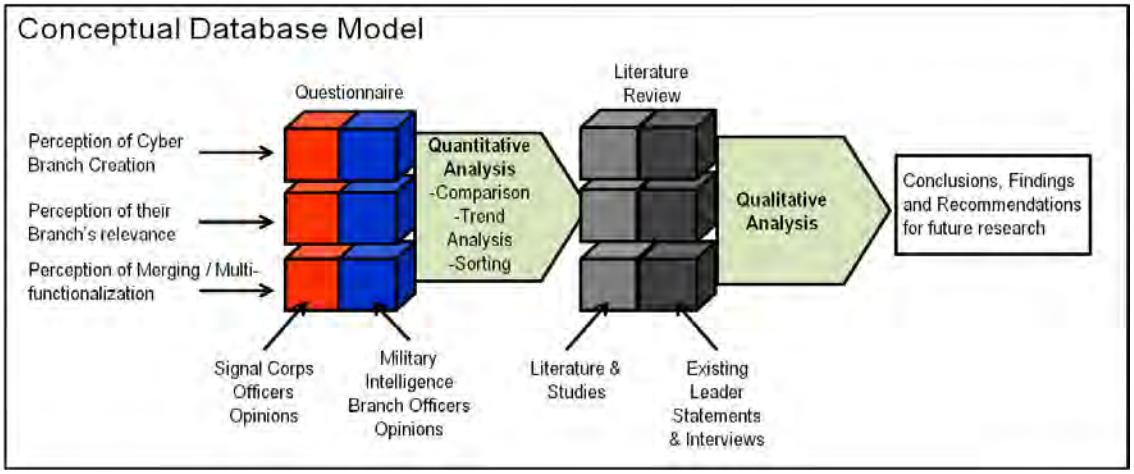


Figure 7. Conceptual Database Design Model

Source: Created by author.

Instrument Supporting this Research

The survey instrument for this research is an online administered questionnaire, consisting of three parts. The first section is a series of multiple choice questions focused on collecting relevant demographic data from the survey participants. Survey participants are limited to selecting one answer from each data field, and must complete each demographic question prior to advancing to the next. The demographic data collected includes the following categories: Sex of the participant, participant's basic branch, branch detail status, and commissioning source. The intent of collecting demographic data was to determine if the various demographic subsets illustrate trends related to the officer's perceptions.

The second section of the questionnaire consists of a series of two Likert scale tables focused on accessing the participant's perceptions. The first Likert scale assesses participant perceptions concerning the future of their respective branch, the impact of the

creation of the Cyber Branch on both the Army and their basic branch, and their assessment of the officer's perception of their and their peer group's ability to lead cyber forces. The second Likert scale directly assesses the participants' perception of a variety of Signal Corps, Military Intelligence and Cyber Branch merger options.

The final section of the questionnaire is for the participant to elaborate on the research question with anything they feel is relevant to the research. The final section is intentionally open ended to solicit contextual data from the survey participants. Inquisite online survey software was utilized to construct and administer the survey instrument.

Benefits and Limitations of the Survey Instrument

Internet based surveys offer several benefits. First, conducting the survey over a web-based application eliminates researcher interaction with survey participants reducing researcher induced bias. Internet based surveys also increases anonymity, likely encouraging more honest responses. Finally internet based surveys leverage technology to increase the speed of data collection and reduce the burden on survey participants.

Internet based surveys also have several limitations. First online surveys do not allow participants to provide nuanced responses, or to elaborate on their choices. Additionally since the researcher can not observe participants non-verbal indicators are not observed and participants are not able to ask the researcher for clarification. Internet based surveys are dependant on technology, and on the participant's access to the internet. Finally the researcher has no way of determining the level of truthfulness displayed by participants.

Survey Administration

The survey instrument was built in the Inquisite Survey Builder computer program. The Inquisite Survey Builder, a licensed software for creating research surveys, facilitated the creation of an online questionnaire which could be administered to the targeted sample population in a secure and reliable manner. The Inquisite Survey Builder program was provided to the researcher by the CGSC Quality Assurance Office (QAO). The QAO also provided the researcher with access to the Allegiance Engage platform, a computerized system for collecting and analyzing online survey results. The Allegiance Engage platform was utilized to collect and collate the participant's responses to the survey. The survey was created by the researcher and published and administered by the QAO utilizing the Allegiance software. This system of administration eliminated potential researcher induced bias and secured survey response data in accordance with human subjects' protection and Army regulatory requirements. The researcher was provided a digital e-mail roster containing the e-mails of the 130 prospective participants by the CGSC registrar's office. The e-mail roster was provided to the QAO who utilized the Allegiance software to convert the participant's e-mail address in to a unique code. The QAO authenticated the survey and distributed an invitation to participate in the research via the e-mail roster. The unique code assigned to each potential participant was utilized to determine which had completed the survey and which invitees had not. The QAO then used this information to send a reminder e-mail to potential participants, who had not yet completed the survey. Once participants had completed the survey their results were collated by the Allegiance Program and provided to the researcher by the QAO. Survey participants' e-mail addresses and names did not appear on any of the

reports provided to the researcher. The anonymity provided by this process guaranteed participant confidentiality in accordance with human protection policy. Additionally the level of participant confidentiality should have encouraged participants to respond honestly to the survey questions. Informed consent was gained from survey participants and participants had the ability to decline overall participation at any time. Survey participants also had the ability to decline to answer any individual survey question while completing the survey. To gain informed consent the researcher must provide potential participants with information about the survey's purpose, administration, and confidentiality. In accordance with ethical research guidelines the researcher must also weigh potential risks and benefits to survey participants and ensure participants understand the potential risks and benefits they may incur.[55] To gain informed consent both the e-mail invitation and the survey introduction page provided the information required. As the QAO was administering the survey the contact information for the QAO was provided in the invitation for participant queries or concerns. The researcher's name and contact information was also included in the invitation for participants preferring to contact the researcher directly. Due to the QAO's management of participant data both the risk and potential rewards to participation in this research were deemed as low. The QAO maintains the data collected during this research for a period of at least three years. The data is stored in a secure data server that is not accessible to personnel outside of the CGSC QAO.

[55] Louis Rea and Richard A. Parker, *Designing and Conducting Survey Research: A Comprehensive Guide,* 3rd ed. (San Francisco, CA: Jossey-Bass, 2005).

Survey Data Analysis

The quantitative data obtained from the questionnaires was analyzed by group and by distinct demographic category. Computer aided data analysis was conducted using the Allegiance Engage platform to simplify the data set and to identify trends within and across the various demographic groups. Narrative responses to the questionnaire (section three) were also analyzed by the researcher to identify trends and reoccurring themes amongst the participants. To identify and eliminate researcher induced bias a review of the data set and findings was conducted by Operations Research—Systems Analysis, analyst Major James A. Jablonski.

Sample Selection

Purpose sampling has been used to select study participants for this research. As this research is specific to Signal Corps and Military Intelligence officer perceptions their populations form the entirety of the sample population. The Cyber Branch is relatively new and the Army is currently accessing the first group of officers who will be commissioned into the Cyber Branch. As such no Cyber Branch officers are currently available for this research. It should be noted that there are officers who are working within the cyber career field in both Army Cyber Command (ARCYBER) and at the Cyber Center of Excellence (Cyber CoE). It is assumed that with the creation of the Cyber Branch the officers currently conducting cyber operations will be transferred to the Cyber Branch. Since this is a non-probability sample it is not determinable who the results of this survey may apply to beyond the sample population. This research focuses on officers attending the United States Army Command and General Staff College (CGSC) at Fort Leavenworth, Kansas, during fiscal year 2015. CGSC attendees were

selected as the sample population for several reasons. First the students at CGSC have a minimum of nine years of service as an officer. Experience is an important factor, as this group of officers has served in the Army long enough to have at least a basic understanding of the Army's organizational principles, guiding factors, and operating constraints. Additionally as students attending CGSC, all participants have a similar knowledge base stemming from the curriculum taught at the school. Also the sample population has completed at least one successful key developmental (KD) assignment at the Company Grade level, demonstrating experience in their particular career field. Finally, the sample population represents aproximently the top 50 percent of their cohort, having been board selected to attend resident CGSC. These factors indicate the officers represented in the sample population have enough knowledge to provide relevant feedback about the topic. The sample is not a statistical representation of the Army at large or of the respective branches in total. The population available to participate in this research sample is illustrated in table 1.

Table 1. Pool of Available Study Participants

	Active Duty	Reserves / National Guard
Cyber (17A)	0	0
Military Intelligence (35A)	76	3
Signal Corps (25A)	47	5
Signal Functional Area (53/24)	2/0	0/0
Totals	125	8
Combined Total available:	133	

Source: Created by author.

Participant Protection and Data Management

Participation in the study is voluntary, and consent to participate may be resended by the participant at anytime. No identifying data or Personally Identifying Information (PII) has been collected from the participants. No demographic data has been collected from demographic subsets with less than ten representative members. This thesis and supporting documentation will be made available to study participants upon its completion. The sampling frame and method of contact for the sample population is maintained by the CGSC Human Research Protections Administrator, and the CGSC Quality Assurance Office. No physical record will be made of individual survey responses. All survey response data has been stored and held by the CGSC Human Research Protections Administrator and the CGSC Quality Assurance Office.

CHAPTER 4

ANALYSIS AND FINDINGS

Chapter 4 is intended to summarize the results of the survey research. The first portion of chapter 4 focuses on the quantitative statistical analysis of the survey data. The second portion of chapter 4 correlates the quantitative data with the qualitative responses to gain a richer understanding of the survey participants' perceptions. The internal consistency of the aggregate survey response data was determined to be sufficiently reliable using Cronbach's alpha. Of the 133 personnel available to be survey participants, three were eliminated. The two functional area 53 officers were eliminated due to their small sample size being a potential identifying factor in violation of Army Regulation (AR) 600-46, Attitude and Opinion Survey Program and Department of Defense Directive (DoDD) 3216.2, Protection of Human Subjects. The researcher was also eliminated from the participant pool to reduce researcher induced bias. E-mail invitations to complete the survey were sent to 130 potential respondents, 40 responded for a response rate of 29 percent. This provides a confidence level of 95 percent with a ± 13 percent margin of error. The 95 percent level of confidence is deemed sufficient to access the sampling error rate to be at an acceptable level. Initial analyses of the aggregate quantitative data revealed that the officers surveyed overwhelmingly (16 (40 percent) strongly agree, 19 (48 percent) agree) view the creation of the Cyber Branch as being positive for the Army. The majority (21 (53 percent) strongly agree, 14 (35 percent) agree) of respondents also feel that their basic branch will remain relevant into the future even after the creation of the cyber branch. Most respondents would disagree with a merger of the Military Intelligence with any other branch. Twenty-one (21) respondents

(54 percent) view a multi-functional merger of the Signal Corps and Military Intelligence Branches negatively (12 (31 percent) negative, 9 (23 percent) very negative) and 23 (59 percent) survey respondents view a merger of the Military Intelligence and Cyber Branches negatively (14 (36 percent) negative, 9 (23 percent) very negative). The Signal Corps and Cyber Branches are viewed by the respondents as the most favorable to a multifunctional merger with 46 percent (18) of participants supporting a multifunctional merger of the Signal Corps and Cyber Branch, while only nine participants (23 percent) view such a merger negatively. Initial analysis of this data indicates that the officers surveyed view the cyber domain to be pertinent to Army operations in the future, and that the Cyber Branch will assist commanders in conducting operations within the cyber domain. The initial analysis also indicates that officers may be more amenable to a multifunctional merger of the Signal Corps and Cyber Branches than to a multifunctional merger of the Military Intelligence and Signal Corps Branches or Military Intelligence and Cyber Branches.

Demographic Assessment of Study Participants

The first portion of the survey was aimed at understanding the demographic make-up of the participant pool. Demographic information was collected; however, race, age, gender, and years of service were not relevant to this research. Basic branch, branch detail status, and source of commissioning were deemed as pertinent population sub-groups for this research. Army component was deemed relevant; however the population of National Guard and Reserve component Soldiers available was inadequate to provide an acceptable level of anonymity for participants. Questions 1 through 4 were aimed at

understanding the demographic subsets represented within the participant pool. Of the 130 potential participants, 40 participants completed the survey. Of those 23 (57 percent) were Signal officers and 17 (43 percent) were Military Intelligence officers. Twelve (12) (30 percent) had been branch detailed and 28 (70 percent) were not. The source of commissioning question revealed 28 (72 percent) were commissioned through the Reserve Officer Training Corps (ROTC), 10 (26 percent) were Officer Candidate School (OCS) graduates, and one (2 percent) was a graduate from the U.S. Military Academy at West Point.

Question 1: What is your basic branch?

Survey question 1was intended to determine the branch of the participant in order to determine if the participant's branch influenced their perception of a multifunctional branch merger, or their perception of the creation of the Cyber Branch as related to the relevance of their branch. No specific conclusions were intended to be drawn from this question; however, it does indicate that slightly more Signal officers chose to participate in this voluntary study. Of the 40 participants 23 (57 percent) were Signal officers and 17 (43 percent) were Military Intelligence officers. There is not a large enough difference between the Signal Corps and Military Intelligence cohort's level of participation to draw conclusions concerning the causality of this difference. Figure 8 illustrates the survey participants' branches.

Figure 8. Question 1: What is your basic branch?

Source: CGSC Survey, Control Number 15-02-027.

Question 2: Were you branch detailed?

Survey question 2 was intended to examine the experience levels of the surveyed officers as it relates to their current basic branch. Based on their acceptance into CGSC and promotion to major all of the officers surveyed are assumed to have successfully completed at least one key developmental assignment within their basic branch. The completion of a key developmental position constitutes a minimum of base level of experience within the participant's branch. Question 2 is intended to determine if the amount of time and experience an officer gains outside of their basic branch influences their perception of a multifunctionalization of their carrier field. In accordance with DA PAM 600-3 branch detailed officers serve between 12 and 36 months in a combat arms branch at the beginning of their career. It is assumed that the amount of time the officer has spent in their current branch (more for "straight branched" officers, less for branch detailed officers) would influence their perceptions of a multifunctional merger of their

branches. Of the 40 officers surveyed 12 (30 percent) were branch detailed and 28 (70 percent) were not, this is illustrated in figure 9.

Figure 9. Question 2: Were you branch detailed?

Source: CGSC Survey, Control Number 15-02-027.

Of the 12 survey participants who were branch detailed the majority were Military Intelligence officers. Of those participants who were branch detailed nine (9) (75 percent) were Military Intelligence Branch officers and three (3) (25 percent) were Signal officers, this is illustrated by figure 10.

Based on the survey results, there does not appear to be a large divergence of opinions between branch detailed and non-branch detailed officers. Branch detailed officers appear to share a similar set of perceptions to their non-branch detailed peers with the majority of their responses being in line with the overall aggregate of the population.

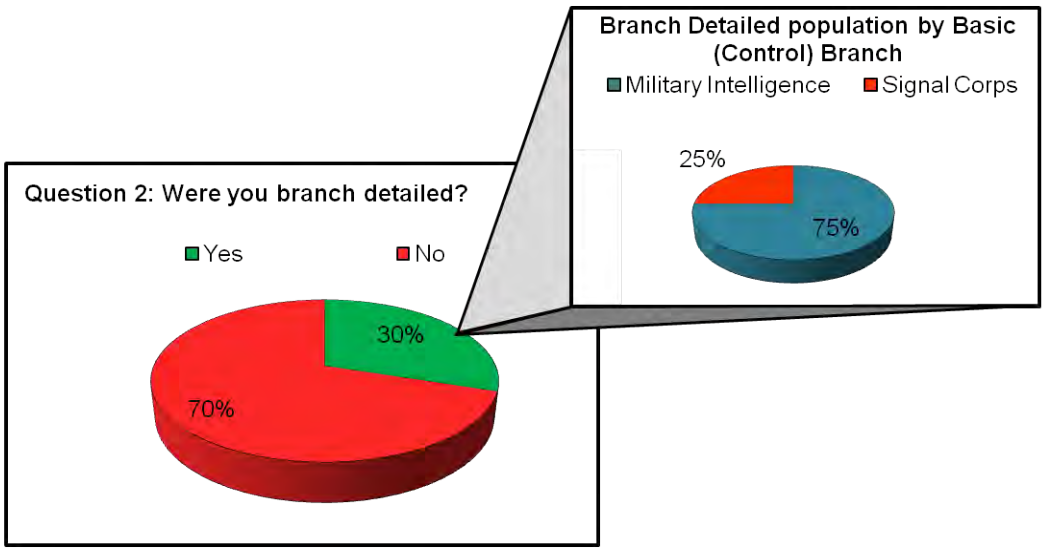


Figure 10. Branch Detailed Participants by Basic (Control) Branch

Source: CGSC Survey, Control Number 15-02-027.

Question 3: What was your commissioning source?

Question 3 is intended to examine if the individual officer's source of commissioning has any bearing on their perceptions of a potential multifunctional merger. For the purpose of this research three commissioning sources were considered: the Reserve Officer Training Corps (ROTC), Officer Candidate School (OCS), and the U.S. Military Academy at West Point. Direct commissioning was not considered as a commissioning source for the purposes of this research. All three of the commissioning sources considered were represented within the sample population. Of the 40 respondents to the survey, 28 (72 percent) were commissioned through the Reserve Officer Training Corps (ROTC), 10 (26 percent) were Officer Candidate School (OCS) graduates, and one (1) (2 percent) was a graduate from the U.S. Military Academy at West Point. The perceptions of the U.S. Military Academy at West Point graduate were considered as part

of the aggregate, but that particular participant was not analyzed as a separate population due to the smaller than acceptable population size. Only the opinions of ROTC and OCS graduates have been accessed comparatively. Figure 11 illustrates the commissioning sources of the survey participants.

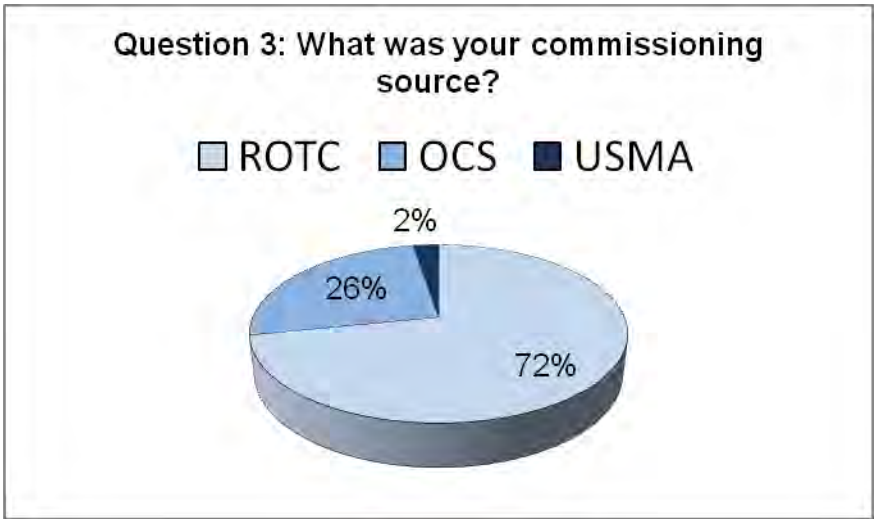


Figure 11. Question 3: What was your commissioning source?

Source: CGSC Survey, Control Number 15-02-027.

Of the 28 ROTC graduates participating in the survey, 16 were branched Signal Corps and 12 were members of the Military Intelligence Branch. Of the 10 OCS graduates, six (6) were members of the Signal Corps and four (4) were branched Military Intelligence. Figure 12 illustrates the participants' branches by commissioning source.

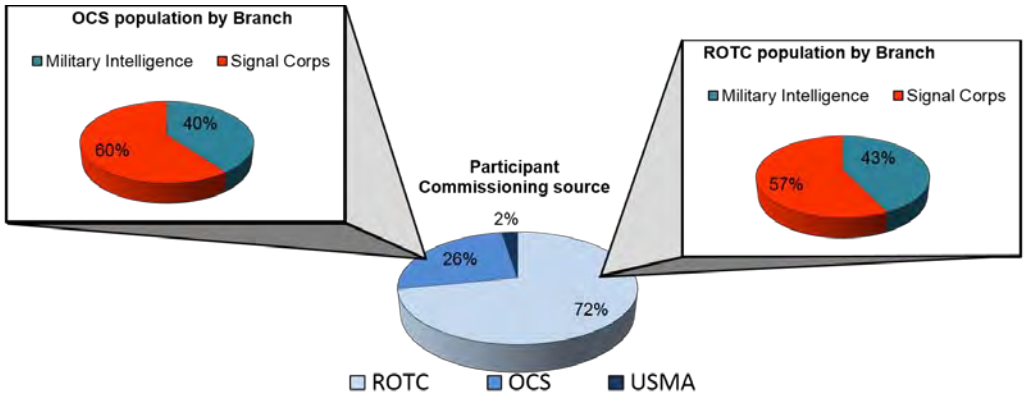


Figure 12. Participants' Branches by Commissioning Source

Source: CGSC Survey, Control Number 15-02-027.

Assessment of Participants' Perceptions

The second and third portion of the survey consisted of Likert scale questions aimed at gaining an understanding of the participants' perceptions. The first scale was intended to glean the participant's perception of the impact of the creation of the Cyber Branch as it relates to the Army at large, commanders in general and their basic branch specifically. The second scale constituted the third portion of the survey and was intended to gain an understanding of the participants' perception of potential multifunctional branch mergers between the Signal Corps, Military Intelligence and Cyber Branches or any combination thereof.

Scale 1: Perceptions of the Creation of the Cyber Branch

In scale participants were asked to indicate their level of agreement with five statements. Participants were able to choose whether they strongly agree, agree, neither agree nor disagree (neutral), disagree or strongly disagree with each statement. The first

two statements were intended to gauge the officer's perception of the impact the creation of the Cyber Branch will have on the Army. Statements one and two were as follows: "The creation of the Cyber Branch will have a positive impact on the Army" and "With the creation of the Cyber Branch, Army leaders can better utilize the cyber domain to accomplish their mission." The remaining three statements from scale one were designed to determine the participant's perception of the creation of the Cyber Branch's impact on their basic branch. Statements three through five were as follows: "With the creation of the Cyber Branch I feel positive about the continued relevance of my basic branch;" "The creation of the Cyber Branch will have a positive impact on my basic branch;" and "Officers in my basic branch are able to lead cyber forces." All 40 survey participants completed scale one.

Survey participants overwhelmingly perceive the creation of the Cyber Branch as having a positive impact on the Army with 88 percent (35) of respondents either strongly agreeing (40 percent) or agreeing (48 percent). Only one respondent disagreed stating: "The individuals that will be great to work in cyber don't have the military attitude and we will limit our effective workforce by require(ing) them to be a soldier." The participant seems to be indicating a perceived cultural difference between typical Soldiers and cyber practitioners. This perceived cultural difference is noted by the proponents of a separate Cyber Service discussed in chapter 2. Both Signal Corps and Military Intelligence officers view the creation of the Cyber Branch as being positive for the Army. 87 percent of Signal officers and 89 percent of Military Intelligence officers indicated agreement to statement one. Both Signal Corps and Military Intelligence officers also agreed that the Cyber Branch will assist commanders to better utilize the

cyber domain to accomplish their mission with 74 percent of Signal officers and 88 percent of Military Intelligence officers agreeing to statement two.

Statements three through five were focused on the participants' perception of the creation of the Cyber Branch's impact on their basic branch. In the aggregate the majority (88 percent) of survey respondents felt that their basic branch will remain relevant into the future. Following the creation of the Cyber Branch, Signal officers appear to be less certain about the future relevance of their branch than are their Military Intelligence counterparts, though the majority of Signal officers did respond positively. 26 percent of Signal officers strongly agreed with statement three, 52 percent agreed with statement three, while 4 percent (1) expressed disagreement. The remainder of the Signal officers (17 percent) chose a neutral or uncertain response. This is contrasted by the Military Intelligence Branch officers unanimous (100 percent) agreement (88 percent strongly agree, 12 percent agree) that their branch will remain relevant following the creation of the Cyber Branch. Signal officers were also much more divided concerning the impact the creation of the Cyber Branch will have on their basic branch, with 39 percent agreeing (4 percent strongly agree, 35 percent agree) that the Cyber Branch will have a positive impact and 26 percent disagreeing that the Cyber Branch will have a positive impact. 35 percent of Signal officers choose a neutral stance. Military Intelligence Branch officers appear much more positive concerning the impact that the Cyber Branch will have on their branch with 82 percent agreeing (41 percent strongly agree, 41 percent agree) with statement four. Both Signal Corps and Military Intelligence Officers were statistically equal in their responses to statement five with 47 percent of members of both

branches agreeing that members of their branch were able to lead cyber forces. Table 2 illustrates the responses to scale 1.

Table 2. Responses to Scale 1

	Aggregate					Signal Corps Officers					Military Intelligence Officers				
	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
The creation of the Cyber Branch will have a positive Impact on the Army.	40%	48%	10%	3%	0%	22%	65%	13%	0%	0%	65%	24%	6%	6%	0%
	16	19	4	1	0	5	15	3	0	0	11	4	1	1	0
	88%		10%	3%		87%		13%	0%		89%		6%	6%	
With the creation of the Cyber Branch, Army leaders can better utilize the Cyber Domain to acomplish their mission.	38%	43%	15%	5%	0%	22%	52%	26%	0%	0%	59%	29%	0%	12%	0%
	15	17	6	2	0	5	12	6	0	0	10	5	0	2	0
	81%		15%	5%		74%		26%	0%		88%		0%	12%	
With the creation of the Cyber Branch, I feel positive about the continued relevance of my basic branch	53%	35%	10%	3%	0%	26%	52%	17%	4%	0%	88%	12%	0%	0%	0%
	21	14	4	1	0	6	12	4	1	0	15	2	0	0	0
	88%		10%	3%		78%		17%	4%		100%		0%	0%	
The creation of the Cyber Branch, will have a positive impact on my basic branch	20%	38%	28%	15%	0%	4%	35%	35%	26%	0%	41%	41%	18%	0%	0%
	8	15	11	6	0	1	8	8	6	0	7	7	3	0	0
	58%		28%	15%		39%		35%	26%		82%		18%	0%	
Officers in my basic branch are able to lead cyber forces	33%	15%	33%	18%	3%	30%	17%	30%	17%	4%	35%	12%	35%	18%	0%
	13	6	13	7	1	7	4	7	4	1	6	2	6	3	0
	48%		33%	21%		47%		30%	21%		47%		35%	18%	

Source: Created by author, CGSC Survey, Control Number 15-02-027.

Demographic Subset Responses to Scale 1

The first demographic subset analyzed was branch detail status. Branch detailed officers are more likely to feel positive about the continued relevance of their basic branch, than their non-branch detailed peers, with 100 percent (12) of the branch detailed

respondents either strongly agreeing 10 (83 percent) or agreeing 2 (17 percent) that they feel positive about the continued relevance of their basic branch. This is in line with the overall tone of survey respondents to that question, with 88 percent of the aggregate of respondents agreeing to feeling positive about the future relevance of their basic branch. Branch detailed officers also are much more positive in their perception of the creation of the Cyber Branch's impact on their basic branch, with 83 percent (10) of branch detailed officers either strongly agreeing (4 (33 percent)) or agreeing (6 (50 percent)) that "Cyber Branch will have a positive impact on their basic branch." This compares to the aggregate of all officers surveyed being much more divided in their opinion with 48 percent (13 strongly agree, 6 agree) and 15 percent (6 disagree). Branch detailed officers are also more likely to believe that officers in their basic branch are able to lead cyber forces with 67 percent of branch detailed officers perceiving that officers in their branch could lead cyber forces, compared to 48 percent of the aggregate who believe the same. Table 3 illustrates the branch detailed and non-branch detailed officer responses to scale 1.

Table 3. Branch Detailed and Non-Branch Detailed Responses to Scale 1

	Aggregate					Branch Detailed					Non-Branch Detailed				
	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
The creation of the Cyber Branch will have a positive Impact on the Army.	40%	48%	10%	3%	0%	58%	25%	8%	8%	0%	32%	57%	11%	0%	0%
	16	19	4	1	0	7	3	1	1	0	9	16	3	0	0
	88%		10%	3%		83%		8%	8%		89%		11%	0%	
With the creation of the Cyber Branch, Army leaders can better utilize the Cyber Domain to acomplish their mission.	38%	43%	15%	5%	0%	50%	33%	8%	8%	0%	32%	46%	18%	4%	0%
	15	17	6	2	0	6	4	1	1	0	9	13	5	1	0
	81%		15%	5%		83%		8%	8%		78%		18%	12%	
With the creation of the Cyber Branch, I feel positive about the continued relevance of my basic branch	53%	35%	10%	3%	0%	83%	17%	0%	0%	0%	39%	43%	14%	4%	0%
	21	14	4	1	0	10	2	0	0	0	11	12	4	1	0
	88%		10%	3%		100%		0%	0%		82%		14%	4%	
The creation of the Cyber Branch, will have a positive impact on my basic branch	20%	38%	28%	15%	0%	33%	50%	17%	0%	0%	14%	32%	32%	21%	0%
	8	15	11	6	0	4	6	2	0	0	4	9	9	6	0
	58%		28%	15%		83%		17%	0%		46%		32%	21%	
Officers in my basic branch are able to lead cyber forces	33%	15%	33%	18%	3%	50%	17%	17%	17%	0%	25%	14%	39%	18%	4%
	13	6	13	7	1	6	2	2	2	0	7	4	11	5	1
	48%		33%	21%		67%		17%	17%		39%		39%	22%	

Source: Created by author, CGSC Survey, Control Number 15-02-027.

The second demographic subset analyzed was the participant's commissioning source. The U.S. Military Academy at West Point was excluded from assessment due to the inadequate size of the population sample. ROTC and OCS graduate responses were similar for the first two statements. 89 percent of ROTC graduates and 90 percent of OCS graduates felt that the creation of the Cyber Branch will be positive for the Army. Of the of ROTC graduates 78 percent, and 90 percent of OCS graduates agreed that the Cyber Branch will enable Army leaders to better utilize the cyber domain to accomplish their

mission. ROTC graduates as a group are more positive about the continued relevance of their respective branches than OCS graduates. 97 percent of ROTC graduates either agree (43 percent) or strongly agree (54 percent) that they are positive about the future relevance of their branch following the creation of the Cyber Branch. Though OCS graduates are also generally positive in their responses to statement 3 with 60 percent either agreeing (20 percent) or strongly agreeing (40 percent), they are seemingly less certain than their peers commissioned through ROTC, with 40 percent of OCS graduates selecting a neutral response, whereas no ROTC graduates selected a neutral response. The majority of ROTC graduates (64 percent) believe that the creation of the Cyber Branch will have a positive impact on their basic branch. The OCS graduates were evenly split in their perception of the Cyber Branch's impact on their basic branch with 30 percent of OCS graduates either agreeing (20 percent) or strongly agreeing (10 percent) that Cyber Branch would have a positive impact on their branch and 30 percent disagreeing with the statement. Most (61 percent) ROTC graduates felt that officers in their basic branch are able to lead cyber forces. OCS graduates appeared to be more uncertain about officers in their branch leading cyber forces with 70 percent choosing to neither agree nor disagree with statement five. Table 4 illustrates survey responses to scale 1 based on commissioning source.

Table 4. ROTC and OCS Commissioning Source
Responses to Scale 1

	Aggregate					ROTC					OCS				
	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
The creation of the Cyber Branch will have a positive Impact on the Army.	40%	48%	10%	3%	0%	39%	50%	11%	0%	0%	40%	50%	10%	0%	0%
	16	19	4	1	0	11	14	3	0	0	4	5	1	0	0
	88%		10%	3%		89%		11%	0%		90%		10%	0%	
With the creation of the Cyber Branch, Army leaders can better utilize the Cyber Domain to acomplish their mission.	38%	43%	15%	5%	0%	39%	39%	18%	4%	0%	30%	60%	10%	0%	0%
	15	17	6	2	0	11	11	5	1	0	3	6	1	0	0
	81%		15%	5%		78%		18%	4%		90%		10%	0%	
With the creation of the Cyber Branch, I feel positive about the continued relevance of my basic branch	53%	35%	10%	3%	0%	54%	43%	0%	4%	0%	40%	20%	40%	0%	0%
	21	14	4	1	0	15	12	0	1	0	4	2	4	0	0
	88%		10%	3%		97%		0%	4%		60%		40%	0%	
The creation of the Cyber Branch, will have a positive impact on my basic branch	20%	38%	28%	15%	0%	18%	46%	25%	11%	0%	20%	10%	40%	30%	0%
	8	15	11	6	0	5	13	7	3	0	2	1	4	3	0
	58%		28%	15%		64%		25%	11%		30%		40%	30%	
Officers in my basic branch are able to lead cyber forces	33%	15%	33%	18%	3%	43%	18%	21%	18%	0%	0%	10%	70%	10%	10%
	13	6	13	7	1	12	5	6	5	0	0	1	7	1	1
	48%		33%	21%		61%		21%	18%		10%		70%	20%	

Source: Created by author, CGSC Survey, Control Number 15-02-027.

Qualitative Analysis of Responses to Scale 1

The survey revealed that participants overwhelmingly perceive the creation of the Cyber Branch will be positive for the Army at large. The survey participants also largely feel that the creation of the Cyber Branch will assist Army leaders to better utilize the cyber domain to accomplish their mission. A Military Intelligence officer expressed the positive perception of the Cyber Branch and seems to be alluding to the relationships

described in Army FM 3-38 *Cyber Electromagnetic Activities* with the statement: "If MI works well with Cyber this can be a very good and productive relationship."

Most Military Intelligence officers perceive that the creation of the Cyber Branch will be positive for their basic branch. One Military Intelligence officer indicated in his statement that the Cyber Branch will alleviate some of the strain on Military Intelligence officers stating: "MI is already at such a breadth and depth of capability that being a 35D has increasingly become self defeating. Cyber Branch will alleviate some of the unrealistic expectations put on the MI corps to be masters of all trades." Another Military Intelligence officer also expressed a positive perception of the Cyber Branch stating: "MI officers will be interested in the Cyber Branch but it will add to not take away from the functions of the branch."

Signal officers were also generally positive concerning the future relevance of their branch. Several Signal officers reflected a positive tone regarding the future relevance of their branch. One Signal officer seems to be reflecting the message of the former commander of the Cyber Center of Excellence, Major General Lawarren Patterson stating: "The Signal Corps will always be required to IOM (install, operate, and maintain) the DoDIN to provide services to the customers." Another Signal Corps officer reflected a positive tone based on the belief that the Signal Corps and Cyber Branches have separate, distinct missions stating: "Signal provides the backbone for communications to travel on. Cyber will utilize that backbone and provide a level of protection on it and use it as a tool to defeat our enemy."

Though generally positive about the continued relevance of their basic branch Signal officers appear more uncertain than their Military Intelligence Branch peers. One such officer expressed concerns about the impact Cyber will have, stating:

> It has been difficult to determine the impact to the Signal Corps (positive, negative, or none) regarding the transformation of the Signal Center of Excellence to the Cyber Center of Excellence. Due to the blending of the two occupational areas, it appears the Cyber CoE may have taken control of the Signal education centers. While the short term impact may not have been noticed, I still question whether the DOTMLPF influence of the Cyber CoE may eventually erode the gains made by a pure Signal CoE. At this point in my career, it's almost a moot point, but for the generation entering the military now, the impact (if there is one) remains to be seen.

Nearly half (48 percent) of the officers surveyed felt that officers in their branch are able to lead cyber forces. Signal Corps and Military Intelligence Branch officers were statistically even in this belief. Participants agreeing with the statement indicate the belief that leading is a universal attribute of officers regardless of branch. One Military Intelligence Branch officer stated: "To lead or to plan can be branch immaterial. What is important is the capacity to learn the technicality of the domain in which one leads or plans. Planning and management are the same regardless of domain." One of the Signal officers also echoed a similar tone stating: "A Signal officer has many of the basic skills to understand cyber and manage resources to lead cyber forces." Other officers selected a more neutral or negative response because they felt that officers in their branch could lead cyber forces if they received additional training. One such Military Intelligence officer expressed this opinion stating: "MI officers are well prepared to understand the interactions of multiple nations as peers and threats as well as having effective leadership and management skills. Cyber technical skills will need to be taught to the MI officers, as these technical skills lend themselves to the Signal Corps more than the MI Corps."

Another Military Intelligence Branch officer agreed stating: "Officers in my basic branch are not trained on cyber threats or methods in order to lead cyber forces. Additional training is required." Military Intelligence officers were not alone in their perception that more training or education would be required to lead cyber forces. A Signal Corps officer expressed a similar belief stating: "To be able to work in the Cyber Branch, my perception is that it will take a lot of professional certifications to be allowed by DISA (Defense Information Systems Agency) or DoD to touch networks. The average Signal officer does not have these certifications."

Summary and Assessment of Scale 1

Scale one revealed several themes that Army leaders may want to consider as the implementation of the Cyber Branch continues. First the officers surveyed overwhelmingly believe that the Cyber Branch will be positive for the Army. This indicates that the efforts of Lieutenant General Cardon and ARCYBER to reach out to CGSC students are having a positive effect on the students' perception of the importance of the cyber domain. The survey also revealed that though Military Intelligence Branch and Signal officers generally believe that their respective branches will remain relevant in the long term, Signal officers are less certain than their peers in the Military Intelligence Branch. It is hypothesized that the loss of cultural artifacts such as the Signal Center of Excellence (now Cyber Center of Excellence) and movement of Signal officers to the Cyber Branch under the Volunteer Transfer Incentive Program (VTIP) have influenced Signal officers' perceptions about the future relevance of their branch. Finally both Military Intelligence and Signal officers believe that they could lead cyber forces;

however any attempt to institute such a program should be coupled with a complementary training or education program.

Scale 2: Perceptions of a Multifunctional Merger

Scale 2 was intended to gauge the participant's level of agreement with a potential multifunctional merger of the Signal Corps, Military Intelligence and Cyber Branches. Participants were asked to indicate whether they would feel very positive, positive, neither positive or negative (neutral), negative or very negative about a series of potential branch multifunctional mergers. The four questions asked were as follows: The four questions asked were as follows: "I would feel____about a multi-functional merger of the Signal Corps and Military Intelligence Branches;" "I would feel____about a multi-functional merger of the Signal Corps and Cyber Branches;" "I would feel____bout a multi-functional merger of the Military Intelligence and Cyber Branches;" and "I would feel____about a multi-functional merger of the Signal Corps, Military Intelligence and Cyber Branches, all three together." Of the 40 survey participants 39 chose to complete scale 2. Table 5 illustrates the responses to scale 2. The responses to scale 2 reveal that as a group the officers surveyed are more favorable to a multifunctional merger of the Signal Corps and Cyber Branches than to any of the other proposed multifunctional merger options. As a collective the survey participants are most opposed to a multifunctional merger of the Signal Corps, Military Intelligence, and Cyber Branches together with 59 percent (23) of respondents replying that they would view such a merger negatively (36 percent) or very negatively (23 percent). As a group Signal officers are more amenable to all multifunctional mergers than their Military Intelligence peers.

Table 5. Comparison of Responses to Scale 2

	Aggregate					Signal Corps Officers					Military Intelligence Officers				
	Very Positive	Positive	Neither Neg Nor Pos	Negative	Very Negative	Very Positive	Positive	Neither Neg Nor Pos	Negative	Very Negative	Very Positive	Positive	Neither Neg Nor Pos	Negative	Very Negative
I would feel ____about a multi-functional merger of the Signal Corps and Military Intelligence Branches	3%	18%	26%	31%	23%	0%	26%	30%	39%	4%	6%	6%	19%	19%	50%
	1	7	10	12	9	0	6	7	9	1	1	1	3	3	8
	21%		26%	54%		26%		30%	43%		12%		19%	69%	
I would feel ____about a multi-functional merger of the Signal Corps and Cyber Branches	13%	33%	31%	18%	5%	17%	35%	26%	22%	0%	6%	31%	38%	13%	13%
	5	13	12	7	2	4	8	6	5	0	1	5	6	2	2
	46%		31%	23%		52%		26%	22%		37%		38%	26%	
I would feel ____about a multi-functional merger of the Military Intelligence and Cyber Branches	3%	24%	18%	37%	18%	0%	30%	22%	39%	9%	7%	13%	13%	33%	33%
	1	9	7	14	7	0	7	5	9	2	1	2	2	5	5
	27%		18%	55%		30%		22%	48%		20%		13%	66%	
I would feel ____about a multi-functional merger of the Signal Corps, Military Intelligence and Cyber Branches, all three together	8%	23%	10%	36%	23%	9%	26%	13%	48%	4%	6%	19%	6%	19%	50%
	3	9	4	14	9	2	6	3	11	1	1	3	1	3	8
	31%		10%	59%		35%		13%	52%		25%		6%	69%	

Source: Created by author, CGSC Survey, Control Number 15-02-027.

Demographic Subset Responses to Scale 2

The first demographic subset analyzed was branch detail status. Of the 40 officers surveyed 12 (30 percent) were branch detailed and 28 (70 percent) were not. The majority of branch detailed officers were in the Military Intelligence Branch. Of those who were branch detailed 9 (75 percent) were Military Intelligence Branch officers and 3 (25 percent) were Signal officers. The survey revealed that branch detailed officers view a potential merger of the Signal Corps and Military Intelligence Branches much more negatively than their non-branch detailed peers. 81 percent (9) of branch detailed officers

perceive such a multifunctional merger negatively (36 percent) or very negatively (45 percent). Comparatively non-branch detailed officers are more divided in their opinions with 43 percent expressing a negative (29 percent) or very negative (45 percent) perception and 29 percent perceiving such a merger positively (4 percent very positive, 25 percent positive). Of the non-branch detailed officers, 29 percent expressed a neutral perception. Both demographic subsets expressed a similar level of support for a multifunctional merger of the Signal Corps and Cyber branches with 45 percent of branch detailed officers and 47 percent of non-branch detailed officers viewing such a merger positively. Branch detailed and non-branch detailed officers also expressed a similar opinion in regards to a multifunctional merger of the Military Intelligence and Cyber branches, with both groups of officers disagreeing with such a merger. 63 percent of branch detailed officers expressed disagreement while 52 percent of non-branch detailed officers would disagree with a Military Intelligence and Cyber Branch merger. Branch detailed officers would disagree with a multifunctional merger of all three branches (Signal Corps, Military Intelligence, and Cyber Branches) with 81 percent of branch detailed officers expressing a negative perception. Non-branch detailed officers were more evenly spread in their opinion of a merger of the three branches with 50 percent viewing such a merger negatively, 36 percent perceiving it positively, and 14 percent taking a neutral stance. Table 6 compares the branch detailed and non-branch detailed officer's responses to scale 2.

Table 6. Comparison of Branch Detailed and Non-branch Detailed Responses

	Aggregate					Branch Detailed					Non-Branch Detailed				
	Very Positive	Positive	Neither Neg Nor Pos	Negative	Very Negative	Very Positive	Positive	Neither Neg Nor Pos	Negative	Very Negative	Very Positive	Positive	Neither Neg Nor Pos	Negative	Very Negative
I would feel ____about a multi-functional merger of the Signal Corps and Military Intelligence Branches	3%	18%	26%	31%	23%	0%	0%	18%	36%	45%	4%	25%	29%	29%	14%
	1	7	10	12	9	0	0	2	4	5	1	7	8	8	4
	21%		26%	54%		0%		18%	81%		29%		29%	43%	
I would feel ____about a multi-functional merger of the Signal Corps and Cyber Branches	13%	33%	31%	18%	5%	0%	45%	36%	9%	9%	18%	29%	29%	21%	4%
	5	13	12	7	2	0	5	4	1	1	5	8	8	6	1
	46%		31%	23%		45%		36%	18%		47%		29%	25%	
I would feel ____about a multi-functional merger of the Military Intelligence and Cyber Branches	3%	24%	18%	37%	18%	0%	9%	27%	36%	27%	4%	30%	15%	37%	15%
	1	9	7	14	7	0	1	3	4	3	1	8	4	10	4
	27%		18%	55%		9%		27%	63%		34%		15%	52%	
I would feel ____about a multi-functional merger of the Signal Corps, Military Intelligence and Cyber Branches, all three together	8%	23%	10%	36%	23%	0%	18%	0%	45%	36%	11%	25%	14%	32%	18%
	3	9	4	14	9	0	2	0	5	4	3	7	4	9	5
	31%		10%	59%		18%		0%	81%		36%		14%	50%	

Source: Created by author, CGSC Survey, Control Number 15-02-027.

The second demographic subset analyzed was the participant's commissioning source. Again the U.S. Military Academy at West Point was excluded from this assessment due to the inadequate size of the population sample. The responses to scale 2 revealed that ROTC and OCS graduates are statistically in agreement in their opposition to a multifunctional merger of the Signal Corps and Military Intelligence Branches with 55 percent (31 percent negative, 23 percent very negative) of ROTC graduates and 40 percent (20 percent negative, 20 percent very negative) of OCS graduates expressing a negative perception of the merger. ROTC graduates and OCS graduates differ in their

perception of a merger between the Signal Corps and Cyber Branches with half (50 percent) of OCS candidates expressing a negative opinion of the potential merger, while 52 percent of ROTC graduates viewing such a merger positively (11 percent very positive, 41 percent positive). ROTC and OCS graduates also differ in their perception of a multifunctional merger of the Military Intelligence and Cyber Branches. Half (50 percent) of OCS graduates would feel positively about such a merger, while their 61 percent of their ROTC counterparts perceive such a merger negatively (46 percent) or very negatively (15 percent). OCS graduates also have a contrary view of a multifunctional merger of the Signal Corps, Military Intelligence, and Cyber Branches. 60 percent of OCS graduates perceive such a merger positively (10 percent very positive, 50 percent positive) in direct contrast to the 63 percent of ROTC graduates whom view such a merger negatively (37 percent negative, 26 percent very negative). No specific causality is readily apparent to describe the difference in perception between the ROTC and OCS graduates. It may be possible that since OCS graduates may have begun their Army careers in other branches they may be more open to transitioning between branches. Additionally OCS graduates have potentially been in the Army longer, and may therefore feel a greater commitment to the Army at large rather than their particular branch. One participant seems to echo this sentiment stating: "I have no issue with a merge. Whatever is best for the bigger ARMY and the sharing of INTEL for the war fighter." Another OCS graduate struck a similarly pragmatic tone stating: "I believe merging the branches could provide utility in reducing the stovepipes/barriers that allow for the effective sharing of information and analysis." Table 7 illustrates the comparison between ROTC and OCS graduates responses.

Table 7. Comparison of ROTC and OCS Commissioning Source

	Aggregate					ROTC					OCS				
	Very Positive	Positive	Neither Neg Nor Pos	Negative	Very Negative	Very Positive	Positive	Neither Neg Nor Pos	Negative	Very Negative	Very Positive	Positive	Neither Neg Nor Pos	Negative	Very Negative
I would feel ____about a multi-functional merger of the Signal Corps and Military Intelligence Branches	3%	18%	26%	31%	23%	0%	19%	26%	33%	22%	10%	20%	30%	20%	20%
	1	7	10	12	9	0	5	7	9	6	1	2	3	2	2
	21%		26%	54%		19%		26%	55%		30%		30%	40%	
I would feel ____about a multi-functional merger of the Signal Corps and Cyber Branches	13%	33%	31%	18%	5%	11%	41%	41%	4%	4%	20%	20%	10%	50%	0%
	5	13	12	7	2	3	11	11	1	1	2	2	1	5	0
	46%		31%	23%		52%		41%	8%		40%		10%	50%	
I would feel ____about a multi-functional merger of the Military Intelligence and Cyber Branches	3%	24%	18%	37%	18%	0%	19%	19%	46%	15%	10%	40%	20%	10%	20%
	1	9	7	14	7	0	5	5	12	4	1	4	2	1	2
	27%		18%	55%		19%		19%	61%		50%		20%	30%	
I would feel ____about a multi-functional merger of the Signal Corps, Military Intelligence and Cyber Branches, all three together	8%	23%	10%	36%	23%	7%	15%	15%	37%	26%	10%	50%	0%	30%	10%
	3	9	4	14	9	2	4	4	10	7	1	5	0	3	1
	31%		10%	59%		22%		15%	63%		60%		0%	40%	

Source: Created by author, CGSC Survey, Control Number 15-02-027.

Qualitative Analysis of Scale 2 Responses

Scale two revealed that the officers surveyed were generally opposed to a multifunctional merger of the Military Intelligence Branch with any of the other branches considered. A Military Intelligence Branch officer summed up the opinion expressed by several Military Intelligence officers stating:

> Signal Corps and the Cyber Branch have multiple characteristics in common; however, the MI branch focuses on a myriad of intelligence collection and analysis that is not covered by either Signal or Cyber. If the Army merges the MI Corps with another branch it is likely to lose significant capabilities due to budget constraints, ex: HUMINT, SIGINT, IMINT, MASINT . . . those INTs have nothing to do with Cyber or the Signal Corps other than utilizing servers and the internet to communicate.

Other Military Intelligence officers highlighted the myriad of fields Military Intelligence officers are expected to have expertise in, feeling that adding expertise in the cyber domain would demand too much of the members of the branch. One officer explained his perception thusly: "I think the MI Branch has a full plate." Another Military Intelligence officer agreed stating: "MI has to do a lot more than just computer stuff. Multifunctional mergers are a simple solution to a complex problem. Our doctrine provides the framework for moving forward: create a doctrinal template of what we need, THEN apply the constraints of the environment. The multifunctional merger reflects the opposite of this process." A third participant succinctly described what they felt a potential problem with multifunctionalization would be stating: "In an already challenging and complex environment asking our Army Officers to be proficient in multiple functional areas do not seem feasible or advantageous."

Even though many participants were opposed to most of the multifunctional merger options, the majority of survey participants would feel positively about a multifunctional merger of the Signal Corps and Cyber Branches. Far more Signal officers support such a merger than Military Intelligence Branch officers. The responses of both Signal Corps and Military Intelligence Branch officers indicate that participants perceive an affinity between the Signal Corps and Cyber Branches, even if they view them as distinctively different. One respondent, a Military Intelligence officer stated: "At the officer level, I believe that Signal and Cyber officers will have a greater chance of interoperability." A Signal Corps officer goes even further stating:

> Looks like a very interesting branch. I think the traditional Signal jobs should become a secondary function of the Cyber Branch. More STEM (science, technology, engineering, and math) officers should be assigned to Cyber/Signal. I

> think that if the Cyber Branch stays the way it is now, it will pigeon hole them to a few jobs in a few posts. A Cyber officer would be marginalized/underutilized at the BDE (Brigade) level.

Another Signal Officer pointed to the Signal officer as being critical to the conduct of successful cyber operations, in a statement which seems to be echoing the concepts described in FM 3-38 *Cyber Electromagnetic Activities*: "Cyber is a great initiative with a tremendous upside for the Army. That being said, there remains a critical link between the cyber domain and the more traditional domains. That link is a good Signal officer."

Other Signal officers felt that having a Cyber Branch separate from the larger Signal Corps was not necessary. One such officer seems to feel that the cyber career field could be a functional area rather than a branch stating: "Cyber looks and feels more like a functional area at this time, it might transition later but for now it looks like a functional area." Another Signal Corps officer seems to feel that the Cyber Branch is not required: "It's an additional layer unneeded. 9/11 displayed how having multiple layers can and still is problematic. We are also creating an additional command structure and staff that is only duplicating what current command and staff structures could absorb and manage." Another Signal Corps officer agreed stating "(I) do not understand the necessity of creating the branch instead of additional MOS's (military occupational specialties) under the Signal Branch. A Signal officer is just as capable of managing a cyber section as he/she is managing a JNN PLT (Joint Network Node Platoon). . . . We would have been better served to have kept the Signal Branch and MI Branches intact and created the additional new MOS's required and placed them under the strategic Signal BNs (Battalions)." In the following comment a different Signal Corps officer explains their

perception that the Military Intelligence Branch and Signal Corps are distinctly separate and that the Cyber Branch is unneeded:

> We should not have created a separate Cyber Branch and instead should have added the capability to the Signal Branch. You could still have CPTs (Cyber Protection Teams) as currently planned and executing. The intel (Military Intelligence) capability would be an addition or an MToE (Modified Table of Equipment) slot or slots as needed. To expect an intel officer to be able to function as a Signal officer or vice versa would require more additional schooling that the Army may not have the time and/or money to pay for. I do not see MI and SC as easily or even moderately interchangeable.

The aforementioned responses reveal that though the respondents acknowledge the importance of maintaining primacy in the cyber domain (based on responses to scale one) a significant portion view the Cyber Branch as duplicating effort, and the cyber career field as being a subordinate element of the Signal Corps.

A portion of the officers surveyed expressed a desire for interested Signal Corps and Military Intelligence officers to receive training, education, and assignment opportunities within the cyber force. One respondent was explicit in expressing the desire to transition between their traditional branch and the Cyber Branch: "I see Cyber Branch and Signal Branch as mutually supporting. My hope is that Cyber Branch allows Signal and Military Intelligence personnel to rotate in and out in KD (key developmental) and staff jobs. The latter two branches offer a unique perspective of the cyber domain." Another officer asks for a path to transition to becoming a cyber operator stating: "I would have loved to transfer into the Cyber Branch but I am completely ignorant in cyber technical skills. If there would have been a transition course, I would have signed up a while ago."

Summary and Assessment of Scale 2

Scale 2 was designed to assess the participants' level of support for a variety of multi-functionalization options. Scale 2 revealed a variety of considerations for Army leaders as they adjust the Army's organizational structure to meet future requirements.

First most officers perceive the Signal Corps and Cyber Branches as being more linked and mutually supportive than the Military Intelligence and Cyber Branches or Military Intelligence and Signal Corps. The Military Intelligence Branch is considered by its members as already being somewhat multifunctional due to the variety of intelligence fields Military Intelligence officers are expected to have expertise in. It is assumed that any effort to combine the Military Intelligence Branch with either the Signal Corps or Cyber Branch would be viewed negatively by officers in that branch.

As a group Signal officers are more amenable to all of the proposed types of multifunctional mergers than their Military Intelligence Branch peers. A merger between the Signal Corps and Cyber Branches was viewed most favorably by the majority of officers surveyed. The perceived linkage between the Signal Corps and Cyber Branches and the desire of a portion of the Signal Corps and Military Intelligence officers to receive training in and be assigned to cyber positions is a key factor Army leaders should consider in making any decision to multifunctionalize Signal Corps, Military Intelligence, or Cyber officers.

Conclusion

The survey instrument was designed to provide both quantitative and qualitative data concerning the survey participants' perceptions about the impact the creation of the Cyber Branch will have and their perceptions of a potential multifunctional merger of

their respective branch with the Cyber Branch. Survey participants indicated an array of responses to the questions asked. Amongst the officers surveyed the creation of the Cyber Branch is perceived to be positive for the Army. The participants also feel that the Cyber Branch will better enable Army leaders to accomplish their mission. The officers surveyed would perceive a merger of the Military Intelligence Branch with any other branch negatively. Participants perceive the Signal Corps and Cyber Branches as being linked and mutually supportive. Signal officers are more likely to support a multifunctional merger with the Cyber Branch than are any other demographic group studied. As Army leaders establish the cyber force and trim the Army to fit current and future budgetary constraints there are several options available to leverage the findings of this study. The researcher's specific recommendations for Army leaders in tackling these challenges are described in detail in the chapter 5.

CHAPTER 5

CONCLUSION AND RECOMMENDATIONS

Summary

As we move forward the cyber workforce will be an increasingly prominent component of America's defense establishment. The Cyber Branch is the Army's current solution to managing its cyber practitioners. Prior to the Cyber Branch two previously existent branches, the Military Intelligence, and the Signal Corps were primarily responsible for operations within the cyber domain. Now that there is a Cyber Branch the role that Military Intelligence and Signal officers will fill in the cyber domain is not clear. The paradigm shift in cyber operations and other cultural factors affect the way Signal and Military Intelligence officers perceive the creation of the Cyber Branch and its anticipated effects. For example, the Voluntary Transfer Incentive Program initiated to build the Cyber Branch, overwhelmingly seeks applicants with the same skill sets and certifications as the Signal Corps. Additionally the transformation of the Signal Center of Excellence to the Cyber Center of Excellence represents a loss of a significant cultural artifact to the Signal Corps. The combined effect of these changes was borne out in the results of this research. Signal officers are less certain about the future relevance of their branch, than are their Military Intelligence peers. Signal officers are also much more likely to feel that the Cyber Branch will be negative for their branch. Beyond accessing the participants' thoughts about the creation of the Cyber Branch this research was also intended to access the participants' perception of a potential multifunctional merger of the Cyber Branch with their branches.

With a reduction in the scale of ground combat operations in Iraq and Afghanistan the DoD and Army are facing severe reductions in their operating budgets and their personnel end strength. Along with an overall smaller budget, the Budget Control Act of 2013, commonly known as sequestration, has led the Army to adjust funding priorities and in the former Secretary of Defense Chuck Hagle's words make "tough, tough choices."[56] As the Army prepares to defend the nation in an environment where budget constraints are normalized, the search for greater efficiency will be more important than ever. A technique the Army may leverage to reduce redundancy and increase efficiency is multifunctionalization of a portion of its officers. The multifunctional logistics program represents a precedent for leveraging a multifunctional approach to gain efficiency. The multifunctional logistics program (FA90) started in 1992 during a similar period of budget and personnel reductions. The program combined Ordnance, Quartermaster, and Transportation officers following their graduation from the Combined Logistics Captain's Career Course (CLC3). As a result of the multifunctional logistics functional area program, and its progeny the Logistics Branch the Army was able to increase the flexibility of Logistics' officer assignments while simultaneously reducing the cost associated with maintaining separate educational, and management facilities. Army leaders may view a similar multifunctional approach to Signal, Military Intelligence, and Cyber officer management as a way to further reduce redundancy and cost.

This research examined how Signal and Military Intelligence officers would perceive a potential multifunctional merger of the Signal Corps, Military Intelligence,

[56] David Alexander, "Big Budget Cuts Pose 'Tough, Tough Choices' for Pentagon: Hagel," *Reuters*, March 6, 2014, accessed November 29, 2014, http://www.reuters.com/article/2014/03/06/us-usa-defense-budget-idUSBREA2500W20140306.

and Cyber branches, in a variety of combinations. The survey revealed two main conclusions based on the participant's responses. First the participants were opposed to a merger of the Military Intelligence Branch with any other branch. Second most participants would support a multifunctional merger of the Signal Corps and Cyber Branches.

The Military Intelligence Branch is viewed as essentially "multifunctional" by its practitioners. Several Military Intelligence officers indicated that they are already required to have a wide breath of knowledge in order to synthesize the various intelligence collection and assessment methods into a coherent intelligence picture. Currently Military Intelligence officers are required to have knowledge of a variety of intelligence disciplines, referred to as "INTs" that represent the various collection and assessment methods within the Military Intelligence field including: Signals Intelligence (SIGINT), Measurement and Signature Intelligence (MASINT), Technical Intelligence (TECHINT), Imagery Intelligence (IMINT), Human Intelligence (HUMINT), Geospatial Intelligence (GEOINT), and Open Source Intelligence (OSINT). The broad scope of what is expected from Military Intelligence officers leads them to feel that their "plate is too full" to assume a leading role within the cyber domain. Military Intelligence officers are more likely to view the cyber domain as a conduit for the collection of intelligence rather than a battlefield within itself. This perception combined with the scope of the Military Intelligence Branch shapes the overwhelming opposition towards any multifunctional merger amongst Military Intelligence officers.

Signal officers are more open to each of the proposed merger options. A multifunctional merger of the Signal Corps and the Cyber Branch is viewed as the most

favorable option by all participants. The technical nature of the Signal Corps and the Cyber Branch, and the fact that both branches have varying degrees of responsibility for the computer and network infrastructure comprising the DoDIN led participants surveyed to view the Signal Corps and the Cyber Branches' missions as mutually supportive and the branches themselves as inextricably linked. This foundational connection combined with other cultural indicators, such as the Cyber Center of Excellence (CoE) residing at Fort Gordon, Georgia, the "home of the Signal Corps" influences the participants' perception that the Signal Corps and Cyber Branch are in essence two sides of the same coin.

Overall Recommendations

First it is recommended that as Army leaders weigh potential options to gain efficiency they consider the opinions and perceptions of midgrade level officers prior to making decisions. Such consideration is essential if Army leaders are to gain a broad base of support for their actions. The Army has a tradition of conducting such research, such as the various Officer Personnel Management System (OPMS) study groups; however recent changes such as the adoption of the Universal Camouflage Pattern and the 2014 revision to AR 670-1, *Wear and Appearance of Army Uniforms and Insignia* seem to have been made without adequate research into soldier's potential perceptions of the proposed changes. This led to costly and highly publicized reversals in both the case of the Universal Camouflage Pattern and the changes to AR 670-1, which may have been avoided with adequate, un-biased research into the soldier's perceptions prior to implementation. With even bigger potential changes to, structure, compensation,

entitlements, and retirement, on the horizon the need for quality research is greater than ever.

It is recommended that the Army consider a pilot volunteer functional area program similar to the FA90 (Multifunctional Logistician) program for interested Signal and Cyber officers. This would allow these officers to remain with their core branch while gaining valuable skills in a complementary career field. These officers would presumably be of more value to the Army because they could fill a greater variety of positions within either cyber or signal billets. Additionally these officers could provide much needed cyber expertise to tactical commanders, who currently do not have authorized cyber operators or organic cyber units. These multifunctional officers could also function as informal educators by training their purely Signal Corps peers and subordinates and by sharing knowledge gained in cyber assignments.

Specific Recommendations pertaining to the Military Intelligence Branch

The Military Intelligence Branch should not be merged with any other branch. Providing relevant, accurate and timely intelligence assessments to commanders at all levels is an essential skill set that a merger could endanger. Additionally, the skills required of Military Intelligence professionals take years to fully develop. Expecting an officer to have adequate skills in both the analytical Military Intelligence field and technical Cyber or Signal fields is unrealistic.

Military Intelligence officers are desirous of receiving more training in how to utilize the cyber domain for intelligence collection. It is recommended that the Army provide Military Intelligence officers with training and education in the Military

Intelligence officer's role in CEMA operations and how to utilize the cyber domain for intelligence collection. To accomplish this, the Army could integrate cyber specific collection training into the Military Intelligence Professional Military Education curriculum. Conversely the Military Intelligence Branch can train cyber practitioners on intelligence collection, intelligence assessment and the targeting process.

The cyber domain is unique in that it crosses several of the traditional intelligence collection and assessment dimensions (SIGINT, MASINT, TECHINT, OSINT, etc.) It is recommended that the Military Intelligence Branch more accurately define which intelligence discipline is primarily responsible for cyber enabled intelligence collection. Alternatively the Military Intelligence Branch may determine that a new "Cyber Intelligence (CYINT)" specialty is needed; however, this is not specifically recommended due to the already diverse nature of intelligence collection.

Specific Recommendations pertaining to the Cyber Branch

First, as the Cyber Branch is a new construct, Army leaders have a unique opportunity to shape the culture that will define the force in the years to come. It is recommended that the leaders of ARCYBER carefully manage the norms, climate, symbology and cultural artifacts associated with the Cyber Branch in order to form a positive branch culture. It is recommended that the leaders of ARCYBER define a cultural vision for the branch, that they communicate their vision to their subordinate leaders, and that they deliberately manage the climate within the force to shape the culture cyber adopts.

Currently there are a variety of industry specific cyber certifications required to become a member of the Cyber Branch. These training and education requirements represent a large cost for the Army in terms of both time and money. It is recommended that the Army work with civilian and government partners in the cyber industry to create a tiered system of required certifications for personnel conducting CEMA, including Military Intelligence and Signal officers. It is also recommended that as the Department of Defense gains cyber capability it create a DoD specific certification, training, and education development path for the members of the Cyber Branch.

It is recommended that in addition to cyber specific training Cyber Branch officers also receive "big picture" training in how the Cyber Branch fits into the overarching Army's construct to support more traditional operations. Such training is especially important as the Cyber Branch's associated civilian workforce may have limited experience with the Army's operating force.

As of now little academic writing has focused on the history of cyber operations, or the creation of the Cyber Branch. It is recommended that ARCYBER appoint a trained unit historian, with the appropriate clearances to record the historically important undertakings of the Cyber Branch. Additionally the Center of Military History (CMH) has an excellent series chronicling the history of the Army's branches. It is recommended that as the Cyber Branch continues to grow important documents relating to its history be forwarded to the CMH staff, where they can be saved for the historical record.

Specific Recommendations pertaining to the Signal Corps

It is recommended that all Signal officers be required to receive a Top Secret clearance prior to graduating from the Signal Corps Captain's Career Course. Currently Signal officers are only required to have a Secret clearance unless their duty position requires them to regularly operate at a higher classification level. Most if not all missions undertaken by ARCYBER are classified at the Secret or Top Secret level. If Signal officers also have a Top Secret clearance they will be equal to their Military Intelligence and Cyber counterparts in the CEMA team. This change would have the added benefit of broadening the pool of Signal officers available for assignment to ARCYBER.

Like their Military Intelligence peers, the Signal officers surveyed want training in CEMA operations. It is recommended that the Cyber Center of Excellence create a "Cyber Leveler Course" similar in function to the former Signal Corps Transition Course, informally referred to as the "levelers course." The Signal Corps Transition Course was a two week intensive course designed to train branch detailed officers on signal operations. Branch detailed officers completed the Leveler Course directly prior to attending the Signal Corps Captain's Career Course. The majority of attendees at the Leveler Course entered having never conducted signal support operations, and graduated with a level of signal knowledge commensurate with their purely Signal Corps branched peers. The proposed Cyber Leveler Course would function in a similar manner; however it would focus on how Signal officers support CEMA, and how Signal officers assist cyber forces in defending the DoDIN. It is recommended that the Cyber Leveler Course be required for all Signal officers, at least until an acceptable base of knowledge exists across the Signal Corps.

In addition to a general cyber familiarization for Signal officers the participants also expressed a desire to receive cyber specific certifications. It is recommended that more opportunities be made available for Signal officers to receive cyber specific certifications. Signal officers could complete the requisite certifications during their professional military education (PME), during broadening and training with industry programs, or even during their operating force assignments.

Specific Recommendations to the Command and General Staff College

Currently signal planning and cyber operations are not taught as a component of the CGSC curriculum. The current curriculum is divided amongst five discrete departments: leadership, history, tactics, joint, multinational and interagency operations, and logistics. Understandably additions to the CGSC curriculum are kept to a minimum to ensure efficient usage of the students' time and government resources. At this time it would likely be too difficult to add additional signal and cyber training to the already packed CGSC curriculum; however, the CGSC staff can still assist in improving the students' knowledge of cyber operations. It is recommended that the CGSC receive instructors with cyber and network defense experience from the Military Intelligence, Signal Corps and Cyber Branches. These officers can serve as subject matter experts for their fellow faculty members, ensure that training scenarios are realistic, and better answer students' questions concerning CEMA.

A greater level of cyber instruction could also be accomplished by leveraging the elective courses available at CGSC. It is recommended that CGSC create Signal Corps and Cyber specific electives and-or elective tracks for Signal Corps and Cyber officers

attending CGSC (Military Intelligence specific electives are existent). CGSC may also leverage opportunities to partner with civilian colleges in the area to create focused cyber security programs students may complete while attending CGSC for Master's Degree credit.

The Masters in Military Art and Science (MMAS) program allows CGSC students to conduct a focused research program on a topic of their choosing. The MMAS thesis is part of a requirement to complete a Master's Degree in Military Art and Science. It is recommended that Cyber Branch, ARCYBER, Signal Corps and Military Intelligence Branch provide CGSC with a list of potential MMAS topics prior to each class. This will cost the branches very little while providing them valuable insight and free data. Additionally the potential gains for the individual student's base of knowledge and self study are immeasurable.

Long Term Recommendations for Army Leaders

Beyond considering a pilot multifunctional Signal—Cyber functional area there are other avenues the Army may want to consider to gain further efficiency well into the future. In the long term it is recommended that the Army consider creating a corps of cyber related officers. For the purposes of this paper the term "Information Dominance Corps" is borrowed from the U.S. Navy, will serve as a name for this corps. It is recommended that this be accomplished by establishing a career group of branches with complementary skill sets similar to the former OMPS career field "Information Operations." This would function similarly to the Navy's Information Dominance

Corps[57] to improve talent management and better manage the career development of Signal Corps, Military Intelligence, Cyber and other related officers. Figure 13 illustrates a potential future revision to the current OMPS.

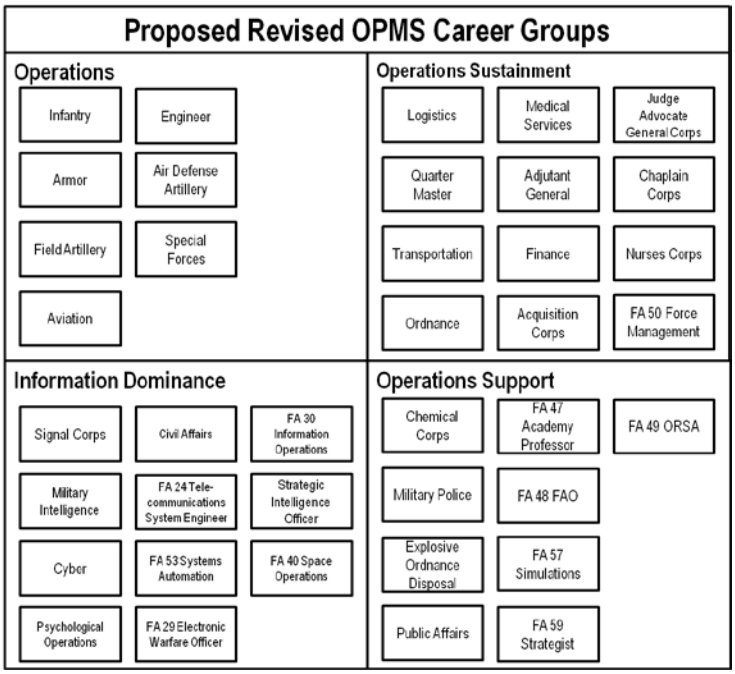


Figure 13. Recommended Revision to the OPMS illustrating the inclusion of an Information Dominance Career Group

Source: Created by author based on recommended changes to the OMPS illustrating the inclusion of an Information Dominance career group.

[57] Navy Information Dominance Corps, "Human Capital Strategy 2012-2017," March 2012, accessed April 9, 2015, http://www.public.navy.mil/fcc-c10f/Strategies/Navy_Information_Dominance_Corps_Human_Capital_Strategy.pdf.

Recommendations for Future Research

There were several areas of inquiry that were tangential to this research where further study would be beneficial to the Army.

The affect that the individual branch specific cultures have on the perceptions of their members has not been adequately researched. The ARCYBER commander, Lieutenant General Cardon referenced the perceived effect of branch culture when he said: "Signal officers want to make the network work . . . they're told make it work SIGO, I don't care how. . . . We have to change that mentality to better defend our networks."[58] There appears to be significant cultural differences among all of the Army's branches, but the reasons why, and the effect of these cultures on the individual officer's decision making, leadership style, and how the officers interact with one another has not been adequately researched.

It is recommended that the Army continue the series of study groups aimed at determining the effectiveness of changes to the OPMS, and Army officer management in general. Talent management is an area where the Army could greatly benefit from research and the OPMS is but one aspect.

More research is required to access how units at the tactical and operational level are conducting CEMA. Currently Cyber Protection Teams (CPT) are the ARCYBER proponent units tasked with defending the DoDIN. The CPTs are not assigned to the division or brigade level as of yet, leaving a potential deficit in protecting tactical level networks from cyber threats. Research into how these units are currently conducting

[58] Cardon, Briefing.

cyber operations, can assist ARCYBER to better defend the Army's premiere maneuver elements' mission command infrastructure.

The budgetary and operational effects of merging the logistics branches are well documented; however little research has been conducted into the perceptions of the logisticians affected by the change to a multifunctional approach. Research into this field can help Army leaders understand the longer term effects of multifunctionalization on the Army's officer corps.

Finally it is recommended that more research be conducted into how the Army and DoD should organize its cyber forces. Each component of the DoD has a slightly divergent structure for its individual cyber forces. Understanding what an optimized cyber organizational structure would be if one exists would greatly benefit the DoD in the future.

Conclusion

The Army is in a potentially historic period of change. The budgetary and personnel constraints the Army will continue to face offer both challenges and opportunities. A multifunctional approach to managing officers is not a panacea for all budgetary woes. The challenge of doing more with less personnel and money will remain; however allowing some Signal Corps and Cyber Branch officers to choose a multifunctional path could be very beneficial for the Army at large, and to those officers as individuals. Regardless of the organizational framework the Army chooses to apply to officer management in the future greater reciprocity between Signal, Military Intelligence, and Cyber practitioners is imperative if the U.S. Army is to remain ahead of its competitors. As members of either of the aforementioned branches the officers owe it

to themselves, their profession, and the nation to build a cohesive team aimed at protecting the nation's vital computer and information network.

GLOSSARY

Cyber counterintelligence. Measures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions. Essentially the term cyber is applied as a modifier to denote that the action, task, or mission occurs or functions within the amorphous Global Information Grid (GIG) or its military sub component the Department of Defense Information Network (DoDIN).

Cyber Electromagnetic Activities (CEMA). Activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system.

Cyberspace. A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers.

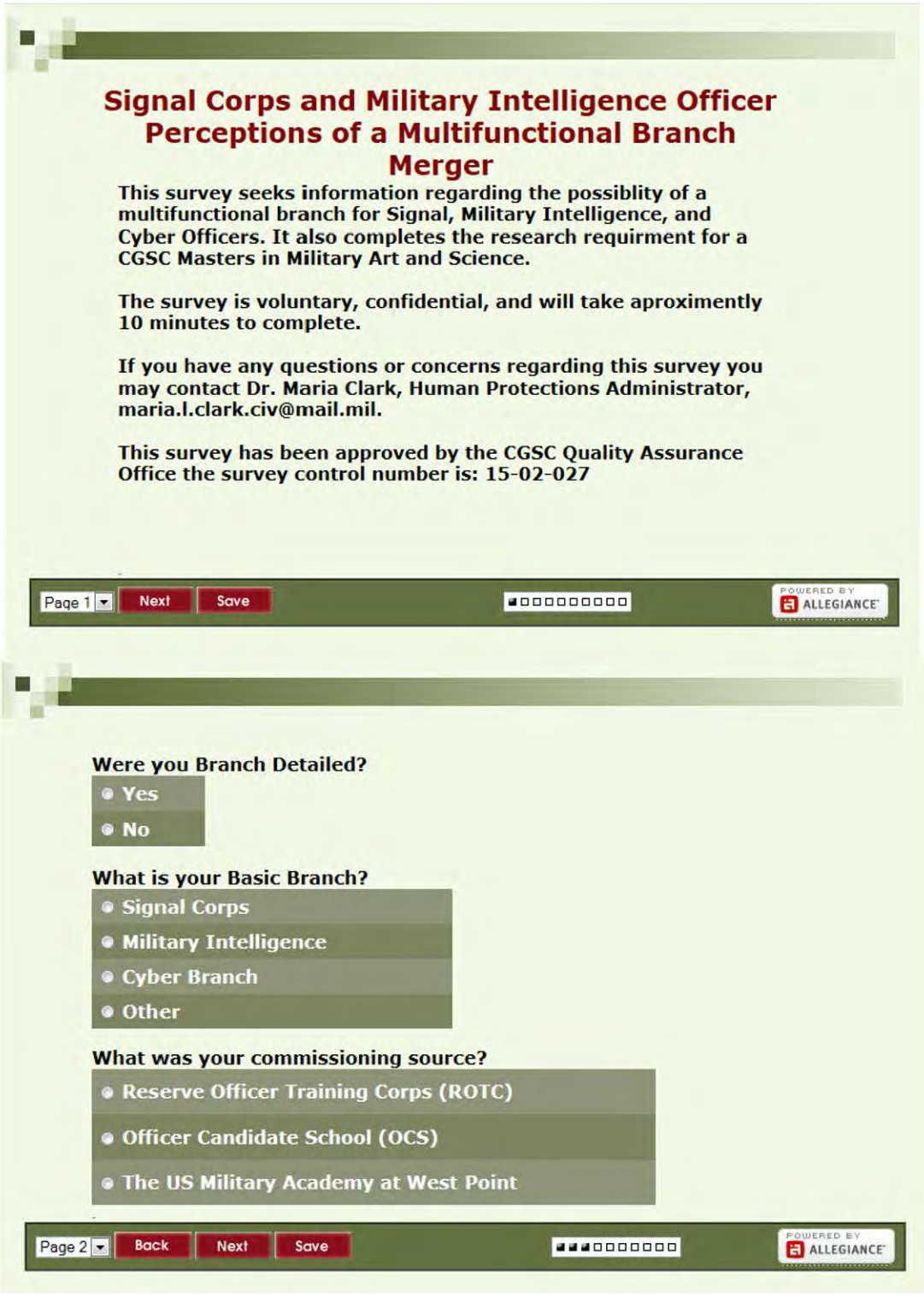
Defensive Cyberspace Operations (DCO). Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net centric capabilities, and other designated systems.

Information environment. The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.

Offensive Cyberspace Operations (OCO). Cyberspace operations intended to project power by the application of force in or through cyberspace.

APPENDIX A

SURVEY INSTRUMENT



Please select your agreement or disagreement with the following statements.	STRONGLY AGREE	AGREE	NEITHER AGREE NOR DISAGREE	DISAGREE	STRONGLY DISAGREE
The creation of the Cyber Branch will have a positive impact on the Army.	○	○	○	○	◉
With the creation of Cyber Branch, Army leaders can better utilize the cyber domain to accomplish their mission.	○	○	○	○	◉

You disagreed that the Cyber Branch will have a positive impact on the Army. Please explain:

You disagreed that Army leaders are better able to utilize the cyber domain as a result of the Cyber Branch creation. Please explain:

Page 3 | Back | Next | Save

POWERED BY ALLEGIANCE

Please select your agreement or disagreement with the following statements.	STRONGLY AGREE	AGREE	NEITHER AGREE NOR DISAGREE	DISAGREE	STRONGLY DISAGREE
With the creation of Cyber Branch, I feel positive about continued relevance of my Basic Branch.	○	○	○	○	○
The creation of the Cyber Branch will have a positive impact on my Basic Branch.	○	○	○	○	○
Officers in my Basic Branch are able to lead Cyber forces.	○	○	○	○	○

Please provide your comments regarding your Branch in relation to the created Cyber Branch.

Page 4 | Back | Next | Save

POWERED BY ALLEGIANCE

Please select the words that best complete the following statements.	Very Positive	Positive	Neither Positive or Negative	Negative	Very Negative
I would feel _____about a multi-functional merger of the Signal Corps and Military Intelligence Branches.					
I would feel _____about a multi-functional merger of the Signal Corps and Cyber Branches.					
I would feel _____about a multi-functional merger of the Military Intelligence and Cyber Branches.					
I would feel _____about a multi-functional merger of the Signal Corps, Military Intelligence, and Cyber Branches all three together.					

Comments regarding multi-functional mergers:

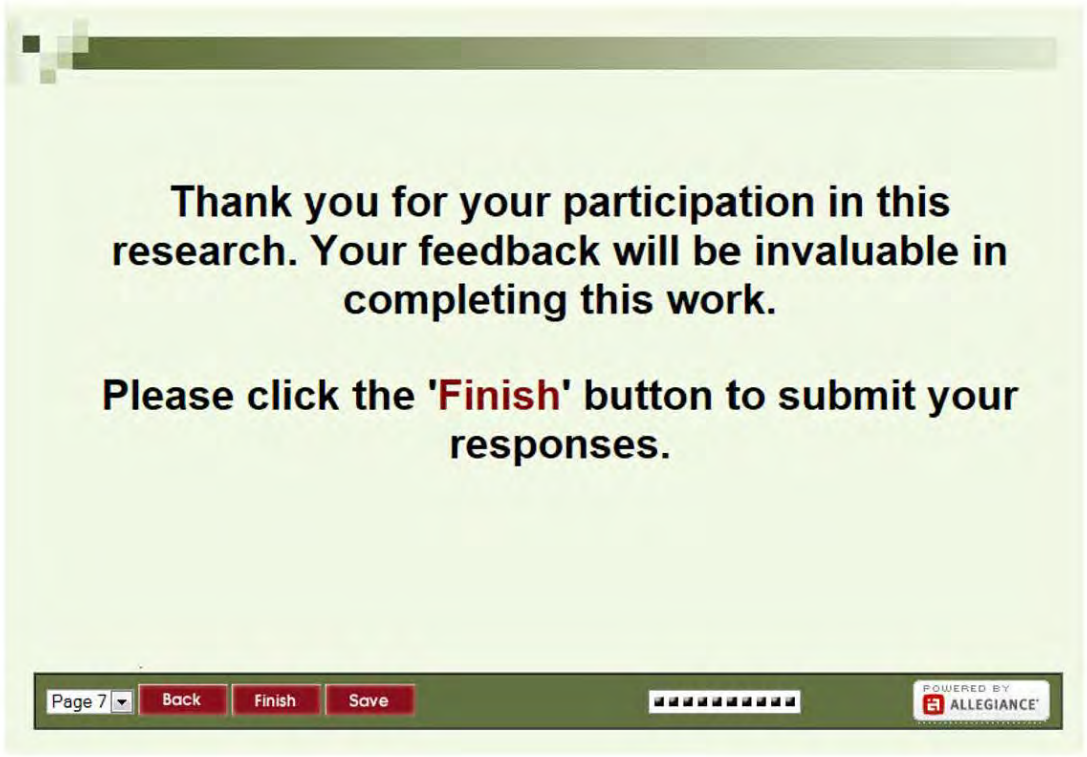
Page 5 Back Next Save

POWERED BY ALLEGIANCE

Please add anything else you would like the researcher to know about Cyber Branch:

Page 6 Back Next Save

POWERED BY ALLEGIANCE


Thank you for your participation in this research. Your feedback will be invaluable in completing this work.
Please click the 'Finish' button to submit your responses.
Page 7
Back
Finish
Save
POWERED BY
ALLEGIANCE

APPENDIX B

SOURCES BY CYBER ORGANIZATIONAL CONCEPT

General Cyber Organizational Topics

Porche III, Isaac R., Christopher Paul, Michael York, Chad C. Serena, Jerry M. Sollinger, Elliot Axelband, Endy M. Daehner, and Brudde J. Held. *Redefining Information Warfare Boundaries for an Army in a Wireless World.* Santa Monica, CA: Rand Corporation, 2013.

Rodriguez, Stephen M., Maj. U.S. Marine Corps. "USCYBERCOM: A Centralized Command of Cyberspace." Research Paper, Naval War College, New Port, RI, 2011.

Woodburn, Clifford M., Maj. U.S. Army. "Leader Development of Cyber Soldiers through Mission Command." Master's Thesis, U.S. Army Command and General Staff College, Fort Leavenworth, KS, 2013.

Cyber Branch

Lieb, Brian J. "Operationalizing Army Cyber." Strategy Research Project, U.S. Army War College, Carslile Barracks, PA, 2013.

Separate Cyber Service

Denny, Eric J. Col. U.S. Air Force. "The Cyberspace Domain: Path to a New Service?" Monograph, School of Advanced Military Studies, Fort Leavenworth, KS, 2013.

Conti, Gregory, and John Surdu. "Army, Navy, Air Force, and Cyber: Is it Time for a Cyberwarfare Branch of Military." *IAnewsletter* 12, no 1 (Spring 2009). Accessed December 15, 2015. http://iac.dtic.mil/iatac.

Cyber Career Field Alignment

Navy Information Dominance Corps. "Human Capital Strategy 2012-2017." March 2012. Accessed April 9, 2015. http://www.public.navy.mil/fcc-c10f/Strategies/Navy_Information_Dominance_Corps_Human_Capital_Strategy.pdf.

Thibodeaux, Maxell S. "Organizing The Army For Information Warfare." Strategy Research Project, U.S. Army War College, Carlisle, PA, 2013.

Cyber Service Like COCOM

Paul, Christopher, Isaac R. Porche III, and Elliot Axelband. *The Other Quiet Professionals, Lessons for Future Cyber Forces.* Santa Monica, CA: Rand Corporation, 2014.

Schosek, Kurt, LTC, U.S. Army. "Military Cyberspace: From Evolution to Revolution." Strategy Research Project, U.S. Army War College, Carlisle, PA, 2012.

BIBLIOGRAPHY

Ackerman, Robert K. "Cyber Commander Calls For Consolidated Activities." *Signal.* June 12, 2013. Accessed October 30, 2014. http://www.afcea.org/content/?q=node/11185.

Alexander, David. "Big Budget Cuts Pose 'Tough, Tough Choices' for Pentagon: Hagel." *Reuters*. March 6, 2014. Accessed November 29, 2014. http://www.reuters.com/article/2014/03/06/us-usa-defense-budget-idUSBREA2500W20140306.

Arnold, Todd, Rob Harrison, and Gregory Conti. "Professionalizing The Army's Cyber Officer Force." Report, Army Cyber Institute, West Point, NY, 2013.

———. "Towards A Career Path In Cyberspace Operations For Army Officers." *Small Wars Journal*, August 18, 2014. Accessed September 2, 2014. http://smallwarsjournal.com/jrnl/art/towards-a-career-path-in-cyberspace-operations-for-army-officers.

Bernstein, Lewis Ph.D. Email received by author, January 30, 2015.

Billingsley, Joseph L. "An Inovation Framework Applied to a Military Cyber Professionals Association." Thesis, Naval Postgraduate School. Monterey, CA, 2013.

Boyce, Paul. "Army Anounces Logistics Branch." The Official Homepage of the United States Army. December 13, 2007. Accessed October 29, 2014. http://www.army.mil/article/6566/Army_Announces_Logistics_Branch/.

Brickey, Jon, Jacob Cox, Jay Nelson, and Gregory Conti. "The Case for Cyber." *Small Wars Journal*, September 13, 2012. Accessed September 3, 2014. http://smallwarsjournal.com/13223.

Cardon, Edward C., U.S. Army Cyber Command. "Cyber Briefing." US Army Command and General Staff College, Fort Leavenworth, Kansas, December 3, 2014.

Combined Arms Support Command. "History of CASCOM." April 15, 2014. Accessed Febuary 24, 2015. http://www.cascom.army.mil/about/history/index.htm.

Department of Defense. *Base Closure and Realighnment Report,* Volume 1, Part 2 of 2 Detailed Recommendations. Washington, DC: Department of Defense, 2005.

Day, Christopher L. "Training for Transformation: When Should the Army Train Multifunctional Logistics?" Master's thesis, Command and General Staff College, Fort Leavenworth, KS, 2003.

Denny, Bryan E. "The Evolution and Demise of U.S. Tank Destroyer Doctrine in the Second World War." Master's thesis, Command and General Staff College, Fort Leavenworth, KS, 1990.

Donnelly, William M., Ph D. "Professionalism and the Officer Personnel Management System." *Military Review* (May-June 2013): 16-23.

Dyess, Anthony T. "Multifunctional Logistics: Comparing Airforce and Army Constructs." Monograph, School of Advanced Military Studies, Fort Leavenworth, KS, 2003.

FAS Military Analysis Network. "Branch." July 26, 1999. Accessed November 23, 2014. http://fas.org/man/dod-101/army/unit/branch.htm.

Fasana, Kenton G. "Using Capabilities to Drive Military Transformation: An Alternative Framework." *Armed Forces and Society* 37, no. 1 (January 2011): 141-162. Accessed November 10, 2014. http://afs.sagepub.com/content/37/1/141.

Harris, Beverly C. "Perceptions of Army Officers in a Changing Army." Research Report 1662, Army Research Institute for the Behavorial and Social Sciences, Alexandria, VA, 1994.

Headquarters, Department of the Army. Department of the Army Pamplet 600-3, *Commissioned Officer Professional Development and Career Management*. Washington, DC: Headquarters, Department of the Army, 2005.

———. Department of the Army Pamplet 600-3, *Commissioned Officer Professional Development and Career Management*. Washington, DC: Headquarters, Department of the Army, 2010.

———. Draft Supplement to Department of the Army Pamplet 600-3, *Commissioned Officer Professional Development and Career Management*. Washington DC: Headquarters, Department of The Army, 2014.

———. Field Manual (FM) 3-38, *Cyber Electromagnetic Activities.* Washington, DC: Headquarters, Department of the Army, 2014.

Johnson, Robert Dr. *Analytic Culture in the US Intelligence Community: Ethnographic Study*. Washington, DC: The Center for the Study of Intelligence, 2005.

Joint Chiefs of Staff. *Capstone Concept for Joint Operations: Joint Force 2020.* Washington, DC: Joint Chiefs of Staff, 2012.

Juskowiak, Terry E. "FA90: An Update on the Multifunctional Logistician Program." *Army Logistician* (November-December 2004): 1-6.

Kolouch, Stephen J. “Retaining Army Engineer Officers.” Monograph, School of Advanced Military Studies, Fort Leavenworth, 2010.

Kurz, Joseph R., LTC, USA. “Sustainment Essentials of the Persain Gulf War.” *Army Sustainment* 44, no. 1 (January-Febuary 2012). Accessed Febuary 24, 2015. http://www.almc.army.mil/alog/issues/JanFeb12/Sustainment_ Essentials.html.

Lieb, Brian J. “Operationalizing Army Cyber.” Strategy Research Project, US Army War College, Carslile Barracks, PA, 2013.

McHugh, John M. General Orders No. 2014-63, *Establishment of the United States Army Cyber Branch*. Washington, DC: Headquarters, Department of the Army, August 21, 2014.

Navy Information Dominance Corps. “Human Capital Strategy 2012-2017.” March 2012. Accessed April 9, 2015. http://www.public.navy.mil/fcc-c10f/Strategies/ Navy_Information_Dominance_Corps_Human_Capital_Strategy.pdf.

Patterson, LaWarren V. “Army turning Signal Center of Excellence into Cyber CoE.” *C4ISR and Networks.* Editor Barry Rosenberg. August 25, 2014. Accessed November 28, 2014. http://www.c4isrnet.com/article/20140801/C4ISRNET07/ 308010002/Army-turning-Signal-Center-Excellence-into-Cyber-CoE.

Paul, Christopher, Isaac R. Porche III, and Elliot Axelband. *The Other Quiet Professionals: Lessons for Future Cyber Forces.* Santa Monica, CA: Rand Corporation, 2014.

Rea, Louis, and Richard A. Parker. *Designing and Conducting Survey Research: A Comprehensive Guide.* 3rd ed. San Francisco, CA: Jossey-Bass, 2005.

Rostker, Bernard. *Right-Sizing the Force, Lessons for the Current Drawdown of American Military Personnel.* Washington, DC: Center for a New American Security, 2013.

Seffers, George L. “Signal Corps is Here to Stay.” *Signal*, September 9, 2014. Accessed November 28, 2014. http://www.afcea.org/content/?q=node/13438.

Stenfors, Vickie D., Major. “The Logistics Officer Corps: Growing Logistics Pentathletes for the 21st Century.” *Army Logistician* 38, no. 5 (September-October 2006). Accessed Febuary 24, 2015. http://www.alu.army.mil/alog/issues/ SepOct06/pentathletes.html.

Strassmann, Paul A. “Bringing Together Signal and Cyber.” *Signal* 68, no. 1 (September 2013): 63-64.

Thibodeaux, Maxwell S. “Organizing The Army For Information Warfare.” Strategic Research Project, US Army War College, Carlisle, PA, 2013.

Thirtle, Michael R. *Educational Benefits and Officer-Commissioning Oportunities Avalable to U.S. Military Servicemembers.* Santa Monica, CA: RAND Corporation, 2001.

Trochim, William. M. *Research Methods Knowledge Base.* October 20, 2006. Accessed November 23, 2014. http://www.socialresearchmethods.net/kb/survtype.php.

United States Army Center of Military History. “Army Birthdays.” November 15, 2004. Accessed December 9, 2014. www.history.army.mil/faq/branches.htm.

United States Army Combined Arms Center. “Command and General Staff College, Mission, Vision, Priorities and Princibles.” October 17, 2014. Accessed November 26, 2014. http://usacac.army.mil/organizations/lde/cgsc/mission.

United States Army War College. “Study on Military Professionalism.” U.S. Army War College, Carlisle Barracks, PA, 1970.

Vandergriff, Donald E. *The Path to Victory: America's Army and the Revolution in Human Affairs.* Novato, CA: Presidio Press, 2002.

Wagner, Martin S. “Multifunctional Logistics Officer Corps: Should the U.S. Army Consolidate the Officer Corps of the Transportation, Quatermaster, and Ordnance Corps Into One Multifunctional Branch?” Monograph, School of Advanced Military Studies, Fort Leavenwoth, KS, 2000.

Waterman, Richard. E. “Perceptions of Sucessfull Field Grade Officers Concerning the Retention Impact of Selected Army Programs and Policies.” Research Project, Army War College, Carlisle Barracks, PA, 1987.

Wemlinger, John V., COL. “The Army's Multifunctional Logistics Units: Can They Support The Joint/Combined Warfighting Effort?” Report, The US Navy War College, College of Naval Warfare, Newport, RI, 1994.

Williams, Brett. “Cyberspace: What is It, Where is It, and Who Cares?” *Armed Forces Journal.* March 1, 2014. Accessed November 23, 2014. http://www.armedforces journal.com/cyberspace-what-is-it-where-is-it-and-who-cares/.

Zetter, Kim. “An Unprecedented Look at Stuxnet, the Worlds First Digital Weapon.” *Wired*, March 11, 2014. Accessed January 21, 2015. http://www.wired.com/ 2014/11/countdown-to-zero-day-stuxnet/.